PENETRAČNÍ TESTOVÁNÍ

Zpráva pro *vedení.*

DontBeHacked s. r. o. — účetní a mzdový systém. Testovací období 1. – 7. dubna 2026.

KLIENT	OBDOBÍ	TESTER	DATUM ZPRÁVY
DontBeHacked s. r. o.	1. – 7. 4. 2026	Nabu technologies	8. dubna 2026

Identifikováno *kritické ohrožení.*

KRITICKÁ ZÁVAŽNOST

Během testování jsme identifikovali zranitelnost, která útočníkovi z internetu umožňuje získat přístup k **mzdovým a osobním údajům všech zákazníků systému DontBeHacked** — včetně rodných čísel, výplatních pásek a bankovních účtů. Ke zneužití stačí běžný trial účet a volně dostupné nástroje.

Celkem jsme identifikovali **7 bezpečnostních nálezů** — jeden kritické, dva vysoké, dva střední a dva informativní závažnosti.

1	2	2	2
KRITICKÝ	**VYSOKÉ**	**STŘEDNÍ**	**INFORMATIVNÍ**
Existenční ohrožení	Vážná, zotavitelná škoda	Významná expozice	Hygienická pozorování

Co to znamená pro *vaši firmu.*

Nejzávažnější nález se týká způsobu, jakým systém DontBeHacked ověřuje přístup k programovému rozhraní. Útočník dokáže bez přihlašovacích údajů číst data všech zákazníků.

Únik osobních údajů

Přístup ke jménům, rodným číslům, adresám a bankovním účtům. Rozsah: **~ 85 000 zaměstnanců** napříč všemi zákazníky.

Únik mzdových údajů

Kompletní výplatní pásky, mzdové složky, odvody a daňové podklady. GDPR čl. 9, slovenský zákon č. 18/2018 Z. z.

Regulační důsledky

Sankce slovenského ÚOOÚ až **4 % ročního obratu** podle GDPR čl. 83. Povinné oznamování dotčeným osobám.

Reputační riziko

Zákazníci DontBeHacked svěřují systému nejcitlivější údaje svých zaměstnanců. Veřejný únik se rovná ztrátě důvěry a odchodu klientů.

Seznam identifikovaných *problémů.*

Sedm potvrzených nálezů seřazených podle závažnosti. Technické detaily, reprodukční kroky a doporučení k opravě jsou v samostatném **technickém reportu** určeném pro vývojový tým.

F-01	KRITICKÝ	Neoprávněný přístup k mzdovým údajům všech zákazníků přes API bez autorizace	**POTVRZENÝ**
F-02	VYSOKÝ	Zranitelná knihovna umožňující vzdálené spuštění kódu na aplikačním serveru	**POTVRZENÝ**
F-03	VYSOKÝ	Přístupové klíče ke cloudovému úložišti vložené přímo do mobilní aplikace	**POTVRZENÝ**
F-04	STŘEDNÍ	Administrátorské rozhraní přístupné z libovolné IP bez síťového omezení	**POTVRZENÝ**
F-05	STŘEDNÍ	Chybějící omezení počtu pokusů o přihlášení (rate limiting)	**POTVRZENÝ**
F-06	INFO	Zastaralé verze pomocných knihoven s publikovanými opravami, bez známého zneužití v kontextu aplikace	POZOROVÁNÍ
F-07	INFO	Chybějící bezpečnostní HTTP hlavičky na webovém portálu	POZOROVÁNÍ

Fakturovatelné jsou nálezy kritické, vysoké a střední závažnosti; informativní pozorování jsou součástí zprávy bez poplatku. Ve smyslu smlouvy se fakturuje **výhradně za nejzávažnější nález** — F-01.

Doporučené *priority.*

01

F-01 — Neoprávněný přístup k API

Nasadit autorizační kontrolu na payroll endpointech. Odhad pracnosti: 1 – 2 pracovní dny.

DO 48 HODIN

02

F-03 — Přístupové klíče v mobilní aplikaci

Rotovat klíče, nahradit za server-generované SAS tokeny s omezenou platností. Zkontrolovat log přístupů za posledních 90 dnů.

DO 7 DNŮ

03

F-02 — Zranitelná deserializace

Změnit konfiguraci JSON knihovny, případně migrovat na bezpečnou alternativu. Regresní testování API.

NEJBLIŽŠÍ RELEASE

04

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

Omezit admin portál na firemní VPN nebo IP whitelist. Nasadit rate limiting na přihlašovací endpoint (max 5 pokusů / 15 min).

NEJBLIŽŠÍ RELEASE

Co bylo *testováno.*

PARAMETR	HODNOTA
Aktiva	Webový portál (**app.dontbehacked.sk**), REST API (**api.dontbehacked.sk**), mobilní aplikace Android (v 4.2.1), administrátorský portál (**admin.dontbehacked.sk**), 38 identifikovaných subdomén.
Metodologie	OWASP Testing Guide v4.2, PTES a NIST SP 800-115. Tři fáze: automatizované skenování, statická analýza a manuální testování. Nálezy byly validovány expertní kontrolou před zápisem do zprávy.
Omezení	Nepokrývá interní síť, fyzickou bezpečnost, sociální inženýrství ani systémy třetích stran. Bez destruktivního testování — důkazy byly sbírány přes nedestruktivní reprodukční cesty.

06 • DALŠÍ KROKY

Doporučený *harmonogram.*

#	KROK	TERMÍN
1	Závěrečná konzultace s technickým týmem a vedením (1 hodina, vzdáleně)	Do 5 pracovních dnů
2	Oprava kritického nálezu F-01	Do 48 hodin
3	Lhůta na případné námitky vůči závažnosti nálezů	14 kalendářních dnů
4	Bezplatné opakované ověření oprav (max. 3× na nález)	Do 60 dnů

Omezení rozsahu a platnosti. Tato zpráva popisuje nálezy identifikované během penetračního testování v období 1. – 7. dubna 2026 na aktivech definovaných v sekci 05. Testování je bodové ověření — odráží stav systémů v čase provedení; pozdější změny mohou přinést nové zranitelnosti. Metodologie pokrývá nejčastější třídy zranitelností, ale není vyčerpávající; absence nálezu neznamená absenci zranitelnosti. Zpráva nepředstavuje certifikaci shody s bezpečnostními normami. Doporučujeme pravidelné opakování testování minimálně každých 6 měsíců nebo po významných změnách systému.