BRANDEFENSE COUNTRY REPORT · CZECHIA 2026

Brandefense Zpráva o kybernetických hrozbách v Česku 2026

Obecní ransomware, zranitelnosti nultého dne, úniky u dodavatelů a sítě legalizačních účtů napříč českými digitálními službami

Odin by Brandefense
Sledované období: 1. ledna až 26. listopadu 2026 (UTC; nedávný vývoj 12. až 26. listopadu)
Verze 1.0 · Veřejné výzkumné vydání · TLP:CLEAR · 27. listopadu 2026

66 z 250

hodnocených českých domén vykazovalo 27. listopadu 2026 aktuální nabídku přístupových údajů

11

veřejných případových složek pokrývajících potvrzené české výpadky a úniky

50

záznamů o ransomwaru označených pro Česko u 20 vyděračských označení

11,8 mld. Kč

pokusů o české bankovní podvody v 75 637 útocích v Q1 až Q3 2026

OBSAH

Obsah

Translated with AI

Přeloženo pomocí AI z anglického originálu. V případě rozdílného znění má přednost anglická verze.

01	Manažerské shrnutí a priority obránců	05
	Mapa zprávy	09
02	Národní digitální profil a prostředí roku 2026	10
03	Národní expozice a pozorování vybraných domén	17
04	Tvrzení a případy z podsvětí	28
05	Veřejné incidenty, dodavatelé a nedávný vývoj	40
06	Výpadky, hacktivismus a tvrzení versus realita	48
07	Ransomware, varování před špionáží a profily hrozeb	52
08	Podvody, zneužití identity a druhotné škody	64
09	Bankovnictví, silná autentizace a kontinuita plateb	70
10	Regulace, ohlašovací povinnosti a řízení	75
11	Výhled a podmíněné spouštěče pro rok 2027	79
12	Akční plán obránců a referenční tabulka nápravy	82
A	Příloha A. Metoda, rozsah a vyloučení	89
B	Příloha B. Registr důkazů	91
C	Příloha C. Zdroje	92
D	Příloha D. Slovníček pojmů	97
	O této zprávě	99

Vedení / Představenstvo / CISO	01 02 05 11 12
SOC / Threat intelligence	03 04 06 07 12.2
Obecní a veřejné IT	03 05 06 10 12
Maloobchod / Banky / Podvody	04 08 09 10 12
Právní / Compliance / DPO	05 08 10 A

O tomto vydání

Přeloženo pomocí AI. Tato česká verze je přeložena z anglického originálu. Důkazy a omezení doprovázejí každé zjištění.

48/100

Národní souhrnná hodnota Atlas pro 250 hodnocených českých domén (snímek 27. listopadu 2026)

53 404

Příspěvků v podsvětí označených pro Česko (1. ledna až 26. listopadu 2026; 64,7 % v srpnu až říjnu)

50

Záznamů o ransomwaru označených pro Česko (1. ledna až 26. listopadu 2026; 27 za celý rok 2025)

11,8 mld. Kč

Pokusů o bankovní kyberpodvody v Q1 až Q3 2026 (75 637 útoků; ztráta 2,2 mld. Kč)

Obsah a čtenářské trasy

Kapitola	Otázka
1 Manažerské shrnutí	Která zjištění a rozhodnutí vyžadují akci vedení jako první?
2 Národní profil	Jak digitální závislost, oficiální trendy a vlna legalizačních účtů tvarují obraz hrozeb?
3 Národní expozice	Která pozorování přihlašovacích údajů, zařízení a poštovních politik vyžadují ověření?
4 Tvrzení z podsvětí	Co skutečně dokládají inzeráty, poptávky a recyklované databáze?
5 Veřejné incidenty	Které veřejně potvrzené události a oznámení dodavatelů zasáhly Česko?
6 Výpadky a hacktivismus	Jak si stojí tvrzení ve srovnání s oficiálními záznamy a skutečným dopadem?
7 Ransomware a aktéři	Co dokládají záznamy vyděračských skupin a varování před špionáží?
8 Podvody a identita	Jak uniklé osobní údaje a služby z podsvětí pohánějí podvody?
9 Bankovnictví a silná identita	Jak útočníci cílí na Bank iD, klienty bank a legalizační účty?
10 Regulace	Který úřad, portál, spouštěč a zákonná lhůta platí v Česku?
11 Výhled	Které měřitelné spouštěče by měly změnit obranný postoj?
12 Akční plán	Kdo jedná, v jakém termínu a s jakým důkazem o splnění?
Přílohy A–D	Rozsah, registr důkazů, zdroje a definice

KAPITOLA 01

Manažerské shrnutí a priority obránců

01

TATO KAPITOLA ODPOVÍDÁ

Které signály roku 2026 vyžadují okamžitou akci českých obránců?

5

hlavních zjištění opřených o oddělené datové soubory

1.1 Pět zjištění pro vedení 06

1.2 Čtyři okamžitá rozhodnutí vedení 07

1.3 Rozsah a hranice této zprávy 07

KAPITOLA 01

Manažerské shrnutí a priority obránců

VE ZKRATCE

Česko vstoupilo do roku 2026 s novým zákonem o kybernetické bezpečnosti (zákon č. 264/2025 Sb.). Současně čelilo obecnímu ransomwaru, kritickým chybám PHP a WordPressu, únikům u dodavatelů a 11,8 miliardy Kč v pokusech o bankovní podvody. Objem příspěvků v podsvětí vyskočil v srpnu až říjnu kvůli ruskojazyčným a ukrajinskojazyčným chatům s legalizačními účty, nikoli kvůli průnikům do bank. Zápla-tujte PHP, WordPress, Citrix a routery ještě dnes, ověřte offline zálohy a oddělte ochranu klientů od obrany perimetru.

1.1 Pět zjištění pro vedení

1. Chyby webových technologií a okrajových zařízení rychle zasáhly české instituce v průběhu roku 2026. Kritický řetězec chyb WordPressu (`CVE-2026-63030`, CVSS 9,8, s `CVE-2026-60137`) stál v srpnu za osmi revidovanými významnými českými incidenty [S8][S15][S63][S77][S78]. Kritické chyby PHP (`CVE-2026-109618`, `CVE-2026-109619`) udeřily v říjnu [S17][S74][S75]. Vyvolaly zhruba dvouhodinovou preventivní odstávku webu Úřadu vlády ČR, omezení služeb Českého hydrometeorologického ústavu (ČHMÚ) a zásah proti aktivnímu útoku na Českém vysokém učení technickém (ČVUT) [S48][S49][S50]. Dříve Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) upozornil na více než 3 200 českých zařízení v botnetu REDHEBERG VNC [S6]. NÚKIB také popsal aktivní obranný zásah Vojenského zpravodajství proti zneužívání routerů TP-Link skupinou APT28 (`CVE-2023-50224`) [S7][S61][S84].

2. Ransomware narušil české obce a obchodní pobočky a offline zálohy pomohly obnově. Potvrzené útoky zasáhly městské úřady v Jemnici, Židlochovicích, Náměšti nad Oslavou a Šumperku [S37][S38][S39][S40][S41]. Kyberútok zpřístupnil i údaje klientů nebankovních dcer Partners (později uvedených vyděračskou skupinou) a koncem listopadu zasáhl ransomware 173 poboček PRO-DOMA [S42][S43][S57]. Ransompedia zaznamenala **50 českých záznamů** u 20 označení oproti **27** za celý rok 2025 [S2]. Pět záznamů, odpovídajících čtyřem potvrzeným veřejným českým případům (Partners Financial Services dvakrát), se shoduje s veřejnými zprávami, zatímco **45 zůstává neověřených** [S2]. Offline zálohy v Náměšti nad Oslavou a pásky v PRO-DOMA umožnily obnovu bez výkupného [S40][S57].

3. Dodavatelé, nástroje zákaznické podpory a starší archivy způsobily rozsáhlé úniky dat klientů a studentů. Bit-Faktura čelila přibližně 38 hodinám neoprávněného přístupu k databázi všech účtů v Polsku a Česku [S44][S45]. Rohlík.cz oznámil zpřístupnění chatů, přepisů hovorů a e-mailů ze zákaznické podpory od dubna do října [S46][S47]. V nedávném období 12. až 26. listopadu oznámila Univerzita Karlova průnik přes webovou aplikaci k datům centrálního Studijního informačního systému (SIS) [S52][S53]. Událost vedla k preventivní výzvě ke změně hesel CAS přibližně pro 55 000 studentů a zaměstnanců [S54]. Samostatně oznámil Dedoles krádež zálohy staršího e-shopu z let 2021 až 2026 přes slovenského IT dodavatele `ui42` [S55][S56].

4. Pokusy o bankovní podvody dosáhly 11,8 miliardy Kč při nárůstu legalizačních účtů na Telegramu. V Q1 až Q3 2026 zastavily banky v Česku **9,6 miliardy Kč (81 %)** pokusů v **75 637 útocích** [S29][S30]. Klienti přesto přišli o **2,2 miliardy Kč** [S29][S30]. Policie zaevidovala **21 137 kybernetických trestných činů** v roce 2025 (+14,3 % meziročně) a

měsíční rekord **2 533 případů** v březnu 2026 [S25][S26]. Souběžně vyskočil objem příspěvků označených pro Česko z 2 470 v červenci na **18 965 v říjnu** (celkem `53 404`) [S1]. Za nárůstem stály ruskojazyčné a ukrajinskojazyčné chaty obchodující s legalizačními účty a poptávající Bank iD a MojeID [S1][S25][S31].

5. Expozice portfolia ukazuje 66 domén s aktuální nabídkou přístupových údajů a nerovnoměrnou obecní hygienu. Napříč všemi 250 hodnocenými českými doménami k 27. listopadu 2026 činí národní souhrnná hodnota Atlas **48/100** [S4]. Aktuální nabídku přihlašovacích údajů vykázalo 66 domén, v čele s maloobchodem (20), vzděláváním (11) a financemi (10) [S4]. V poštovní hygieně publikuje **179 z 250 (71,6 %)** politiku DMARC `quarantine` nebo `reject` a **173 (69,2 %)** publikuje DNSSEC DS včetně všech 25 ústředních domén [S3]. Banky vedou s **23 z 25** vynucujícími doménami, zatímco krajská a obecní správa zaostává na **11 z 25** a **6 bez platného DMARC** [S3].

1.2 Čtyři okamžitá rozhodnutí vedení

1. **Okamžitě záplatujte veřejné webové technologie a okrajová zařízení.** Nasaďte listopadová vydání PHP (`8.5.13`, `8.4.28`, `8.3.37`, `8.2.36` či novější) a opravené verze WordPressu (`6.8.6+`, `6.9.5+`, `7.0.2+`) uvedené v §12.2 [S63][S64][S65][S74][S75][S76][S77][S78]. Aplikujte také aktuální verze Citrix NetScaler (`CTX697305`) a Zimbra a vyřaďte nepodporované routery [S62][S79][S80][S81][S83][S84].
2. **Otestujte obnovu z offline záloh a papírový záložní provoz.** Navazujte na zkušenosti z Náměště nad Oslavou, Židlochovic a PRO-DOMA pravidelným ověřováním neměnných či páskových záloh offline a nácvikem provozu bez živých IT systémů [S39][S40][S57].
3. **Proveďte audit přístupů dodavatelů, uchovávání dat v podpoře a vyřazených záloh.** Zmapujte každého externího IT dodavatele, zrušte neaktivní účty a odstraňte osobní údaje z odstavených záloh e-shopů [S44][S46][S55]. Omezte oprávnění webových aplikací k centrálním databázím [S52].
4. **Ověřte registraci podle zákona č. 264/2025 Sb. a hlásicí kanály.** Potvrďte, zda subjekt hlásí NÚKIB (`GovCERT.CZ`), týmu `CSIRT.CZ`, nebo České národní bance (ČNB) podle DORA [S21][S24][S27][S28]. Uzavřete mezery u monitorovacích politik DMARC [S3].

1.3 Rozsah a hranice této zprávy

Každé číslo v této zprávě zůstává svázáno se svou datovou populací, časovým oknem a úrovní důkazů. Hlavní sledované období pokrývá **1. ledna až 26. listopadu 2026** (UTC podle času zveřejnění) napříč příspěvky z podsvětí (`53 404`), záznamy Ransompedia (`50`), zmínkami domén za rok 2026 (`1 334`) a veřejnými událostmi [S1][S2][S4]. V rámci tohoto období je úsek **12. až 26. listopadu 2026** (`1 771` příspěvků, `53` příspěvků na fórech a tři významné veřejné případy) oddělen v §5.3, aby se nedávný vývoj nezaměňoval s celoročním tempem [S1][S52][S55][S57].

Hodnocení expozice Brandefense Atlas i pasivní kontroly (**všech 250 domén**) zachycují stav k **27. listopadu 2026** [S3][S4]. Klouzavé 365denní zmínky domén v chatech a na dark webu pokrývají **27. listopadu 2025 až 26. listopadu 2026** [S4]. Všechna externí varování, české zákony, nařízení EU a mediální zprávy byly ověřeny **27. listopadu 2026**. Neověřená tvrzení a zločinecké seznamy jsou výslovně označeny a organizace jsou jmenovány pouze tehdy, když byly oficiálně potvrzeny a široce publikovány v českých či mezinárodních médiích.

KLÍČOVÉ ZÁVĚRY

01

Zranitelnosti PHP, WordPressu a okrajových systémů spolu s obecním a obchodním ransomwarem určovaly provozní riziko Česka v roce 2026.

02

Nárůst příspěvků v podsvětí v srpnu až říjnu odráží zprostředkování legalizačních účtů na Telegramu, nikoli kompromitaci bankovní infrastruktury.

03

Záplatujte chyby z §12.2, ověřte offline zálohy, zkontrolujte dodavatele a potvrďte hlásicí trasy podle zákona 264/2025 nebo DORA.

Mapa zprávy

Dvanáct kapitol, pět čtenářských tras. Vyberte rozhodnutí odpovídající vaší odpovědnosti a vždy držte zjištění v hranicích jeho důkazů.

Vedení / Představenstvo / CISO	Které incidenty, finanční ztráty a spouštěče určí rozpočet a odolnost pro rok 2027?	01 02 05 11 12
SOC / Threat intelligence	Které inzeráty jsou recyklovaná tvrzení, která CVE vyžadují záplatu a jak si stojí tvrzení proti realitě?	03 04 06 07 12.2
Obecní a veřejné IT	Jak mohou úřady uzavřít mezery v DMARC a offline zálohách při plnění povinností zákona 264/2025?	03 05 06 10 12
Maloobchod / Banky / Podvody	Jak se zneužití Bank iD, smishing, legalizační účty a úniky u dodavatelů mění ve ztráty klientů?	04 08 09 10 12
Právní / Compliance / DPO	Které lhůty platí u NÚKIB, CSIRT.CZ, ČNB (DORA), ÚOOÚ a podle článku 14 EU CRA?	05 08 10 A

KAPITOLA 02

Národní digitální profil a prostředí roku 2026

02

TATO KAPITOLA ODPOVÍDÁ

Jak digitální závislost a institucionální přechod Česka formují plochu hrozeb roku 2026?

94,2 %

penetrace internetu mezi 9,96 milionu uživatelů

2.1 Digitální propojenost, sdílené identity a veřejný kontext 11

2.2 Oficiální tempo hrozeb v Česku od roku 2025 do konce roku 2026 11

2.3 Výklad objemu příspěvků v podsvětí 13

KAPITOLA 02

Národní digitální profil a prostředí roku 2026

VE ZKRATCE

Česko spojuje téměř univerzální používání internetu, rychlé rozšíření Bank iD a exportní průmyslovou základnu se zásadní regulací podle zákona č. 264/2025 Sb. NÚKIB zaznamenal od ledna do října 2026 celkem 215 revidovaných incidentů, zatímco policejní kyberkriminalita dosáhla rekordních měsíčních hodnot. Objem příspěvků v podsvětí mezitím prudce narostl v srpnu až říjnu kvůli ruskojazyčným a ukrajinskojazyčným chatům s legalizačními účty. Filtrujte šablonové inzeráty bílých koňů, aby výstrahy mířily na skutečné české webové, ransomwarové a podvodné hrozby.

2.1 Digitální propojenost, sdílené identity a veřejný kontext

Na začátku roku 2026 mělo Česko při **10,6 milionu** obyvatel celkem **9,96 milionu uživatelů internetu (94,2 % populace)** [S66]. Počet mobilních připojení dosáhl **14,7 milionu (139 % populace)** a počet identit na sociálních sítích **8,08 milionu (76,4 %)** [S66]. Každodenní agenda občanů a firem silně spoléhá na digitální služby jako Portál občana, Datové schránky, `MojeID` a bankovní identitu (`Bank iD`) [S31][S32]. Vysoká míra digitalizace zrychluje vyřizování daní i nákupů, ale činí ze sdílených identitních portálů a velkých e-shopů atraktivní návnady pro napodobování [S31][S32].

Institucionální kalendář roku 2026 přinesl vedle běžného provozu pravidelné ústavní milníky. Po říjnových parlamentních volbách 2025 nastoupila nová vláda a začátkem roku 2026 prošla hlasováním o důvěře, zatímco v říjnu 2026 proběhly obecní a senátní volby [S67]. Dne 7. ledna 2026 vydala Bezpečnostní rada státu oficiální prohlášení k další roli Česka v mezinárodní muniční iniciativě pro Ukrajinu [S36]. O dva dny později zmínily hacktivistické kanály dodávky munice při výhrůžkách českým vládním webům, v průběhu lednové vlny DDoS hlášené NÚKIB [S1][S9][S36].

2.2 Oficiální tempo hrozeb v Česku od roku 2025 do konce roku 2026

Oficiální hlášení NÚKIB, CSIRT.CZ, Ministerstva vnitra (MV ČR) a Úřadu pro ochranu osobních údajů (ÚOOÚ) ukazují zvýšený provozní tlak před rokem 2026 i během něj. Ve své Zprávě o stavu kybernetické bezpečnosti za rok 2025 zaevidoval NÚKIB **203 kybernetických incidentů** (pokles z 268 v roce 2024), z toho **2 velmi významné**, **12 významných** a **189 méně významných** událostí [S5].

Tento přehled roku 2025 zaznamenal čtyři výchozí milníky před naším sledovaným oknem roku 2026. Zaprvé, v květnu 2025 Česko veřejně připsalo průnik do neutajované sítě Ministerstva zahraničních věcí z let 2022 až 2024 skupině **APT31** (uvedeno výhradně jako kontext před rokem 2026) [S5]. Zadruhé, v červenci 2025 mezinárodní operace **Operation Eastwood** pod vedením Europolu narušila infrastrukturu `NoName057(16)` [S5][S85]. Zatřetí, NÚKIB vydal dvě varování roku 2025 týkající se DeepSeek a přenosu dat do Čínské lidové republiky [S5]. Začtvrté, vláda v září 2025 schválila **Národní strategii kybernetické bezpečnosti 2026–2030** [S20].

Od **ledna do října 2026** dosáhly revidované čtvrtletní a říjnové měsíční počty NÚKIB celkem **215 zaevidovaných incidentů** (`Q1: 75` , `Q2: 44` , `Q3: 65` , `říjen: 31`) [S6][S7][S8][S17]. Součet původních měsíčních přehledů činí **218**, protože NÚKIB incidenty ve čtvrtletních přehledech zpětně reklasifikuje [S7][S8]. Konkrétně duben klesl z 18 původních na 16 revidovaných, srpen z 28 původních na 27 revidovaných a jeden incident z Q1 byl později přeřazen do kategorie velmi významných [S7][S8][S12][S15].

Měsíční počty za deset publikovaných měsíců se vyvíjely takto. Q1 zaznamenalo leden **32** (1 významný), únor **23** (2 významné) a březen **20** (4 významné) [S6][S9][S10][S11]. Q2 vykázalo duben **16** revidovaných (18 původně), květen **12** a červen **16** [S7][S12][S13]. Q3 a říjen zaznamenaly červenec **12**, srpen **27** revidovaných (28 původně; 8 významných), září **26** (1 významný) a říjen **31** (5 významných; 4 DDoS) [S8][S14][S15][S16][S17].

Období (2026)	Revidovaný součet NÚKIB	Významné / velmi významné	Hlavní provozní faktory hlášené NÚKIB	Zdroje
Q1 (led–bře)	75	6 významných, 1 velmi významný (reklasifikováno v Q2)	Zimní vlny DDoS (`NoName057(16)` , `ServerKillers`), botnet REDHEBERG VNC (>3 200 českých zařízení), APT28 `Operation Neusploit` (`CVE-2026-21509`)	[S6][S7][S9][S10][S11]
Q2 (dub–čer)	44	6 významných, 0 velmi významných	Zneužívání routerů TP-Link skupinou APT28 (`CVE-2023-50224`) s aktivním zásahem Vojenského zpravodajství, FortiBleed, smishing napodobující Policii ČR, phishing SparkyCarp na Evropské hodnoty	[S7][S12][S13]
Q3 (čec–zář)	65	13 významných (4 čec, 8 srp, 1 zář), 0 velmi významných	Vlna průniků WordPress `wp2shell` (~dvě třetiny Q3 jako Průnik), STORM-2372, LAUNDRY BEAR Zimbra (`CVE-2025-66376`), exploit kit BlueMoon, zadní vrátka Tenda/Zbtlink	[S8][S14][S15][S16]

Období (2026)	Revidovaný součet NÚKIB	Významné / velmi významné	Hlavní provozní faktory hlášené NÚKIB	Zdroje
Říjen	31	5 významných, 0 velmi významných	Vlna PHP2Shell (`CVE-2026-109618` , `CVE-2026-109619`) u veřejných institucí a univerzit, ~polovina Průnik, 4 incidenty DDoS	[S17][S48][S49]
Celkem led–říj	**215**	**30 významných, 1 velmi významný**	**Měřeno během ročního náběhu zákona 264/2025 (součet prvotních měsíčních zpráv: 218)**	[S6][S7][S8][S17]

NÚKIB výslovně varuje před vykládáním výkyvů v roce 2026 jako přímé změny celostátního počtu útoků [S7][S8]. Zákon č. 264/2025 Sb. nabyl účinnosti **1. listopadu 2025**, spustil postupnou registraci s roční implementační lhůtou (ustanovení `§ 15 odst. 4`) a přesunul hlášení v režimu nižších povinností z NÚKIB na `CSIRT.CZ` [S7][S8][S21][S24]. Mimo regulovaný okruh NÚKIB řešil národní tým **CSIRT.CZ** v roce 2025 celkem **3 005 incidentů** (meziroční růst přes 30 %, nejčastěji phishing) [S23]. Dne **24. listopadu 2026** podepsaly CZ.NIC a NÚKIB novou veřejnoprávní smlouvu potvrzující mandát CSIRT.CZ pro subjekty v režimu nižších povinností [S24].

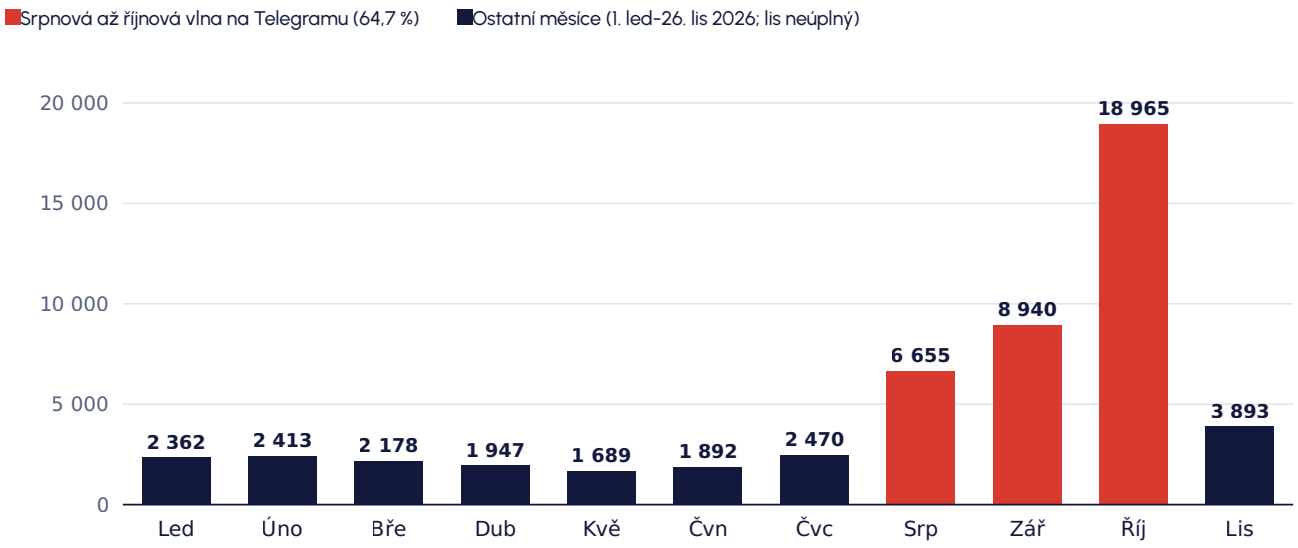
Policejní a ochranářské statistiky ukazují stejným vzestupným směrem. V roce 2025 zaevidovala Policie ČR **21 137 kybernetických trestných činů** (+2 642 případů čili **+14,3 %** meziročně) [S25]. Kyberkriminalita dosáhla **12,4 %** veškeré kriminality, přestože celková kriminalita klesla o 1,9 % [S25]. Objasněnost činila **15,1 %**, přičemž **1 224** případů spadalo pod kvalifikované počítačové trestné činy (ustanovení `§§ 230–232` trestního zákoníku) [S25].

V **březnu 2026** policie zaznamenala měsíční rekord **2 533 případů** (+37 % meziročně), tažený telefonními podvody falešných bankéřů a policistů se škodou **322 milionů Kč** od začátku roku [S26]. Samostatně evidoval ÚOOÚ za rok 2025 historické maximum **392 hlášení porušení zabezpečení osobních údajů** (oproti 336 v roce 2024) spolu s **3 854 podněty** (+68 %) a **1 430 stížnostmi na spam** [S33].

2.3 Výklad objemu příspěvků v podsvětí

Mezi **1. lednem a 26. listopadem 2026** zaznamenal Brandefense **53 404 příspěvků v podsvětí označených pro Česko** [S1]. Měsíční objem zůstal vyrovnaný mezi **1 689 a 2 470 příspěvky** od ledna do července [S1]. Poté prudce vzrostl v **srpnu (6 655)**, **září (8 940)** a **říjnu (18 965)**, než v neúplném období 1. až 26. listopadu klesl na **3 893** [S1]. Dohromady tvoří srpen až říjen **34 560 příspěvků (64,7 %)** celého jedenáctiměsíčního součtu pro Česko [S1].

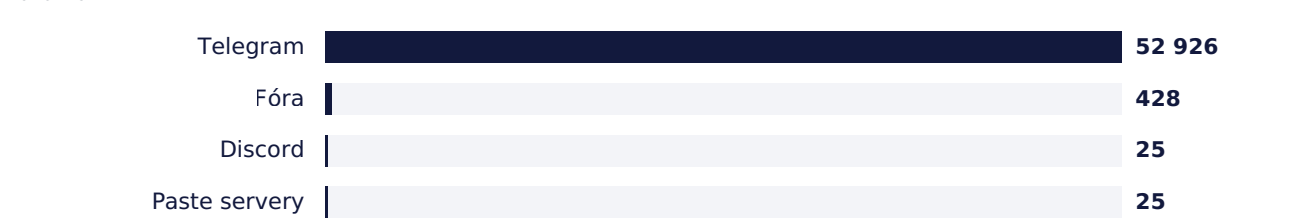
Srpnová až říjnová poptávka po legalizačních účtech na Telegramu tvořila 64,7 % objemu pro Česko



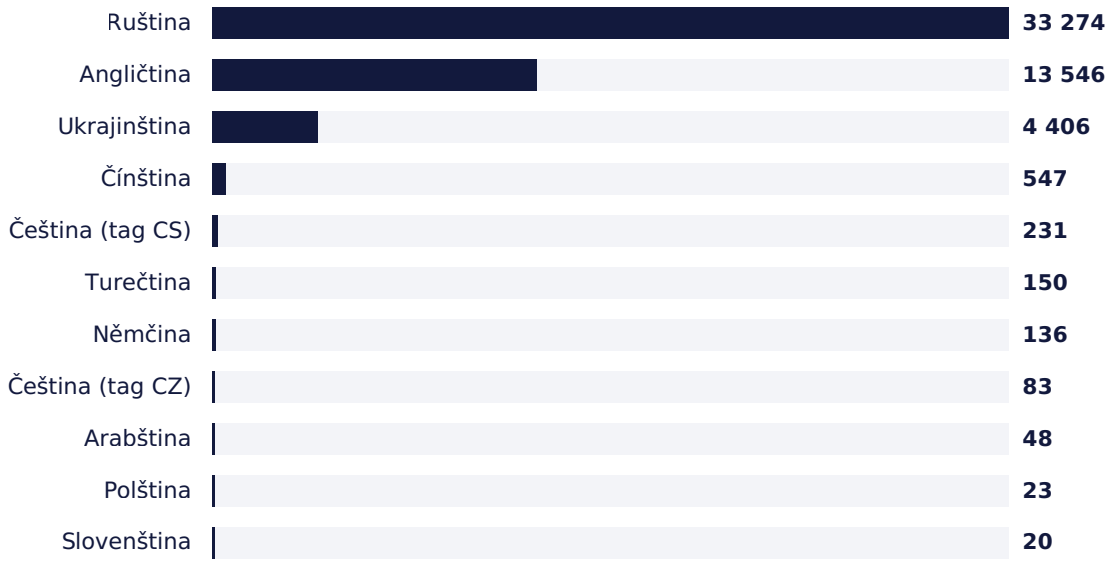
Zdroj: Odin by Brandefense, 53 404 příspěvků v podsvětí označených pro Česko, 1. ledna–26. listopadu 2026; listopad neúplný [S1]. Příspěvky nejsou potvrzené incidenty; jazykové značky se mohou překrývat.

Rozklad podle platforem, jazyků a témat tento nárůst jasně vysvětluje a brání jeho záměně za vlnu průniků do českých firem. Za celé období připadá na **Telegram 52 926 příspěvků (99,1 %)**, následují **fóra (428; 0,8 %)**, **Discord (25)** a **paste servery (25)** při **nule** záznamů na Toru [S1]. Podle jazykových značek (vícejazyčný příspěvek může nést více značek) dominují **ruština (`33 274`)**, **angličtina (`13 546`)** a **ukrajinština (`4 406`)** [S1]. Menší podíl nesou značky **čínština (`547`)**, **čeština (`CS 231` a `CZ 83`)**, **turečtina (`150`)**, **němčina (`136`)**, **arabština (`48`)**, **polština (`23`)** a **slovenština (`20`)** [S1].

Telegram tvoří 99,1 % příspěvků označených pro Česko s převahou ruštiny, angličtiny a ukrajinštiny



Jazyk



Zdroj: Odin by Brandefense, 53 404 příspěvků v podsvětí označených pro Česko, 1. ledna–26. listopadu 2026; listopad neúplný [S1]. Příspěvky nejsou potvrzené incidenty; jazykové značky se mohou překrývat.

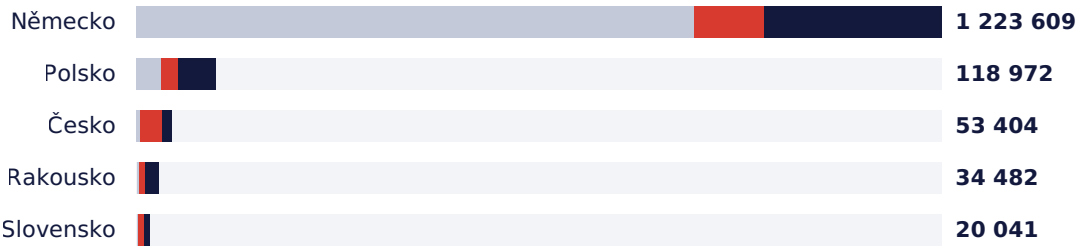
Obsahový rozbor ukazuje, že srpnový až říjnový skok tvoří téměř výhradně **zprostředkování bankovních legalizačních účtů a KYC ověření**, nikoli obchod s firemními průniky [S1]. Příspěvky zaměřené na prodej a pronájem finančních účtů stouply z **458 v červenci** na **2 770 v srpnu**, **6 240 v září** a **13 457 v říjnu** (71,0 % říjnového objemu) [S1]. Tento růst přesně kopíroval říjnová maxima ruštiny (`14 083`) a ukrajinštiny (`2 697`) [S1]. Za celé období se objevilo **28 287 příspěvků o finančních účtech** a **19 599 příspěvků o KYC dokladech** [S1]. Naproti tomu úniky databází tvořily **4 185** příspěvků a nabídky přístupů **2 775** [S1].

Na fórech zahrnuje listopadový nárůst na **101 příspěvků** (z **428**) řadu obecných mezinárodních vláken, která na české organizace necílí [S1]. Skutečné české inzeráty rozebírá kapitola 4 a §5.3 [S1].

Česko se vyhnulo lednové až únorové vlně spamu v Německu, zaznamenalo však vlastní podzimní vlnu na Telegramu



Celkem 1. led–26. lis 2026 (led-úno šedá, srp-říj korálová, ostatní tmavě modrá)



Pouze období srpen–říjen 2026 (samostatné měřítko)



Hrubé příspěvky označené podle zemí napříč sledovanými kanály; nepřepočteno na populaci ani pokrytí zdrojů. Zdroj: Odin by Brandefense, 53 404 příspěvků v podsvětí označených pro Česko, 1. ledna–26. listopadu 2026; listopad neúplný [S1]. Příspěvky nejsou potvrzené incidenty; jazykové značky se mohou překrývat.

Srovnávací země byly vybrány jako příklady výhradně pro poskytnutí kontextu; jejich výběr neznamená žebříček ani politické hodnocení.

Srovnání Česka se čtyřmi bezprostředními sousedy (`Slovensko` , `Polsko` , `Rakousko` a `Německo`) objasňuje měřítko i průběh vln [S1]. Mezi 1. lednem a 26. listopadem 2026 dosáhly celkové počty příspěvků a příspěvků na fórech těchto hodnot: **Česko 53 404 (428 fórum)**, **Slovensko 20 041 (127 fórum)** a **Rakousko 34 482 (320 fórum)** [S1]. Větší sousedé zaznamenali **Polsko 118 972 (726 fórum)** a **Německo 1 223 609 (2 606 fórum)** [S1]. Německo zasáhla masivní zimní vlna hromadného spamu (`429 473` v lednu a `417 736` v únoru) [S1]. Tato vlna Česko minula. Česko naopak zažilo soustředěnou podzimní vlnu ruskojazyčných a ukrajinskojazyčných telegramových chatů s legalizačními účty napojenými na středoevropské trasy praní peněz [S1].

KLÍČOVÉ ZÁVĚRY

01

NÚKIB zaevidoval 215 revidovaných incidentů od ledna do října 2026, zatímco policejní kyberkriminalita a hlášení ÚOOÚ dosáhly rekordních maxim.

02

Srpnový až říjnový nárůst na 18 965 měsíčních příspěvků odráží obchod s legalizačními účty a KYC na Telegramu, nikoli průniky do českých bank.

03

Při třídění výstrah oddělujte zprostředkovatelské chaty bílých koňů a obecná mezinárodní vlákna od ověřených inzerátů na fórech.

KAPITOLA 03

Národní expozice a pozorování vybraných domén

03

TATO KAPITOLA ODPOVÍDÁ

Které signály expozice a mezery v konfiguraci vyžadují ověření u 250 českých domén?

66 z 250

hodnocených českých domén vykazovalo 27. listopadu 2026 aktuální nabídku přístupových údajů

3.1 Složení vzorku a hranice hodnocení 18

3.2 Národní souhrnná hodnota Atlas a aktuální nabídky přístupů 19

3.3 Vazby na infikovaná zařízení a historické záznamy hesel 21

3.4 Dokumenty, podobné domény a 365denní zmínky v podsvětí 24

3.5 Autentizace pošty, DNSSEC, TLS a HSTS u 250 českých domén 24

3.6 Převod signálů expozice do oddělených ověřovacích front 27

KAPITOLA 03

Národní expozice a pozorování vybraných domén

VE ZKRATCE

Napříč všemi 250 hodnocenými českými doménami k 27. listopadu 2026 činí národní souhrnná hodnota Atlas 48/100. Aktuální nabídku údajů vykázalo 66 domén, 221 mělo nejméně 318 706 vazeb na zařízení a 231 mělo 180 747 551 historických záznamů hesel (99,4 % v telekomunikacích a webmailech). Celostátně 71,6 % vynucuje DMARC a 69,2 % podepisuje DNSSEC, ale obce zaostávají na 11 z 25. Prověřte aktuální nabídky do pěti dnů, oddělte firemní zařízení od klientských a uzavřete mezery v DMARC.

3.1 Složení vzorku a hranice hodnocení

Pro vytvoření opakovatelné národní základny bez jmenování soukromých členů portfolia sestavil Brandefense účelový soubor **250 českých domén** rozdělených do **deseti vyrovnaných sektorových skupin po 25 doménách** [S3]. Všech **250** bylo vyhodnoceno k **27. listopadu 2026** [S3][S4]. Deset skupin pokrývá ústřední ministerstva a úřady, krajské a městské úřady, licencované banky a pojišťovny, energetiku, telekomunikace a digitální platformy, velké výrobce, dopravce, nemocnice, univerzity a velké obchodníky [S3].

Parametr portfolia	Hodnota	Provozní význam a hranice	Zdroje
Vybrané a hodnocené domény	250 z 250 (10 skupin × 25)	Účelový národní vzorek, nikoli statistické sčítání všech českých subjektů	[S3][S4]
Národní souhrnná hodnota Atlas	**48/100** (27. listopadu 2026)	Jediná celostátní hodnota expozice; žádná sektorová, skupinová ani firemní skóre nejsou publikována	[S4]
Signály snímku expozice	27. listopadu 2026 (250/250 vyhodnoceno)	Kumulativní signály, které se mohou překrývat; nikdy nevyjadřují unikátní osoby, rok 2026 ani potvrzené incidenty	[S4]
Snímek pasivní konfigurace	27. listopadu 2026 (250/250 vyhodnoceno)	Publikovaný stav DNS, poštovních politik, TLS a HTTP hlaviček k danému datu	[S3]
Klouzavé 365denní zmínky domén	27. listopadu 2025 až 26. listopadu 2026	Zmínky domén v dark chatech a na dark webu; podmnožina 2026 (1. led až 26. lis) odděleně	[S4]

Kapitolu 3 řídí tři přísná interpretační pravidla. Zaprvé, pro celé 250doménové portfolio je publikována jediná národní souhrnná hodnota Atlas (**48/100**); nikde ve zprávě neuvádíme sektorová ani firemní skóre [S4]. Zadruhé, počty expozice (zařízení, historická hesla, dokumenty a podobné názvy) jsou kumulativní vnější pozorování, která

se mohou překrývat a **neprokazují** průnik na server [S4]. Zatřetí, publikované záznamy DNS (`DMARC` , `SPF` , `DKIM` , `DNSSEC` , `CAA`) a publikované stavy TLS/HSTS popisují vnější konfiguraci [S3][S70][S71][S72][S73]. Weby nedostupné k datu snímku uvádíme jako samostatný počet [S3].

3.2 Národní souhrnná hodnota Atlas a aktuální nabídky přístupů

Na snímku k **27. listopadu 2026** činí jediná národní souhrnná hodnota Atlas napříč všemi **250 hodnocenými českými doménami** hodnotu **48/100** [S4]. V portfoliu vykazovalo **66 z 250 domén (26,4 %) aktuální nabídku přihlašovacích údajů** (všech 66 má historii s celkem **5 431 historickými záznamy**) [S4]. Aktuální nabídky představují nejvyšší prioritu k okamžitému ověření vlastníkem, protože ukazují živé nabídky na tržištích odkazující na přihlašovací údaje domény [S4].

Aktuální nabídky přihlašovacích údajů a signály expozice napříč 250 hodnocenými českými doménami

	Aktuální nabídky	Se zařízeními	Zaměstnan. zařízení	S hesly	S dokumenty	Podobné názvy (30 d)
Veřejná správa	1/25	13/25	7/25	15/25	7/25	23/25
Krajská a obecní správa	1/25	22/25	11/25	22/25	10/25	21/25
Bankovnictví a finance	10/25	22/25	16/25	24/25	12/25	22/25
Energetika a utility	4/25	21/25	16/25	25/25	4/25	18/25
Telekomunikace a digitální služby	7/25	25/25	22/25	25/25	15/25	21/25
Průmysl a výroba	0/25	22/25	17/25	22/25	5/25	17/25
Doprava, logistika a pošta	9/25	22/25	14/25	24/25	7/25	22/25
Zdravotnictví a life sciences	3/25	24/25	19/25	24/25	6/25	13/25
Vzdělávání a výzkum	11/25	25/25	24/25	25/25	20/25	22/25
Maloobchod, média a spotřebitelské služby	20/25	25/25	22/25	25/25	15/25	22/25

Aktuální nabídky přihlašovacích údajů podle sektoru (korálová). Každá buňka zobrazuje pozorované domény / 25 hodnocených domén; signály se mohou překrývat. Zdroj: pozorování expozice Brandefense pro všech 250 hodnocených českých domén, snímek k 27. listopadu 2026 [S4]. Kumulativní vazby se mohou překrývat; nepředstavují unikátní osoby ani potvrzené průniky.

Sektorové počty níže ukazují šíři výskytu jednotlivých signálů napříč deseti vyrovnanými 25doménovými skupinami [S4]:

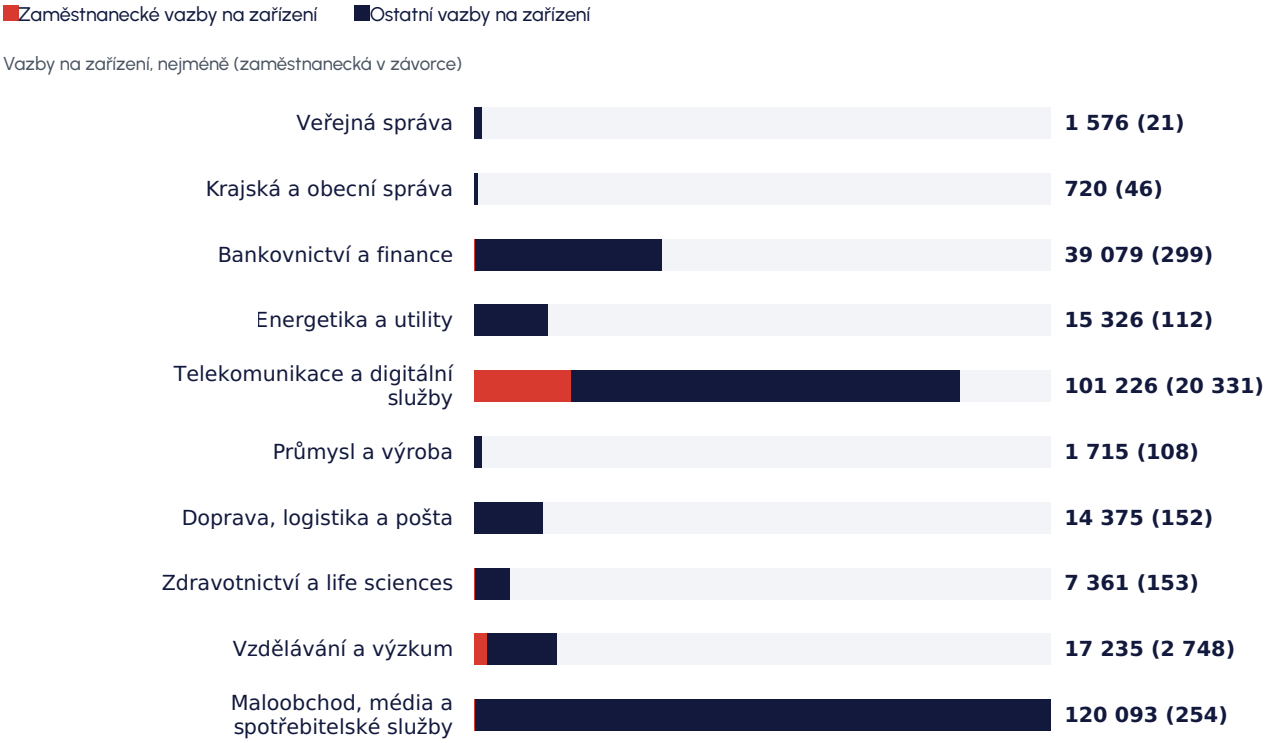
Sektorová skupina (po 25 doménách)	Vyhodnoceno	Domény se zařízeními	Domény se zaměstnaneckými zařízeními	Domény s hesly	Aktuální nabídky přístupů	Historie nabídek	30d podobné názvy	Vystavené dokumenty
Veřejná správa	25	13	7	15	1	1	23	7
Krajská a obecní správa	25	22	11	22	1	1	21	10
Bankovnictví a finance	25	22	16	24	10	10	22	12
Energetika a utility	25	21	16	25	4	4	18	4
Telekomunikace a digitální služby	25	25	22	25	7	7	21	15
Průmysl a výroba	25	22	17	22	0	0	17	5
Doprava, logistika a pošta	25	22	14	24	9	9	22	7
Zdravotnictví a life sciences	25	24	19	24	3	3	13	6
Vzdělávání a výzkum	25	25	24	25	11	11	22	20
Maloobchod, média a spotřebitelské služby	25	25	22	25	20	20	22	15
Celkem	**250**	**221**	**168**	**231**	**66**	**66**	**201**	**101**

Aktuální nabídky přístupů se silně soustřeďují ve velkoobjemových spotřebitelských, akademických a finančních prostředích [S4]. **Maloobchod, média a spotřebitelské služby** vedou s **20 z 25 domén**, následují **Vzdělávání a výzkum (11)**, **Bankovnictví a finance (10)**, **Doprava, logistika a pošta (9)** a **Telekomunikace a digitální služby (7)** [S4]. Naproti tomu **Průmysl a výroba** zaznamenal **nulu aktuálních nabídek**, zatímco **Veřejná správa** i **Krajská a obecní správa** měly po **1 doméně** [S4]. Nabídky v portfoliu nejsou v této zprávě spojeny s žádnou jmenovanou organizací.

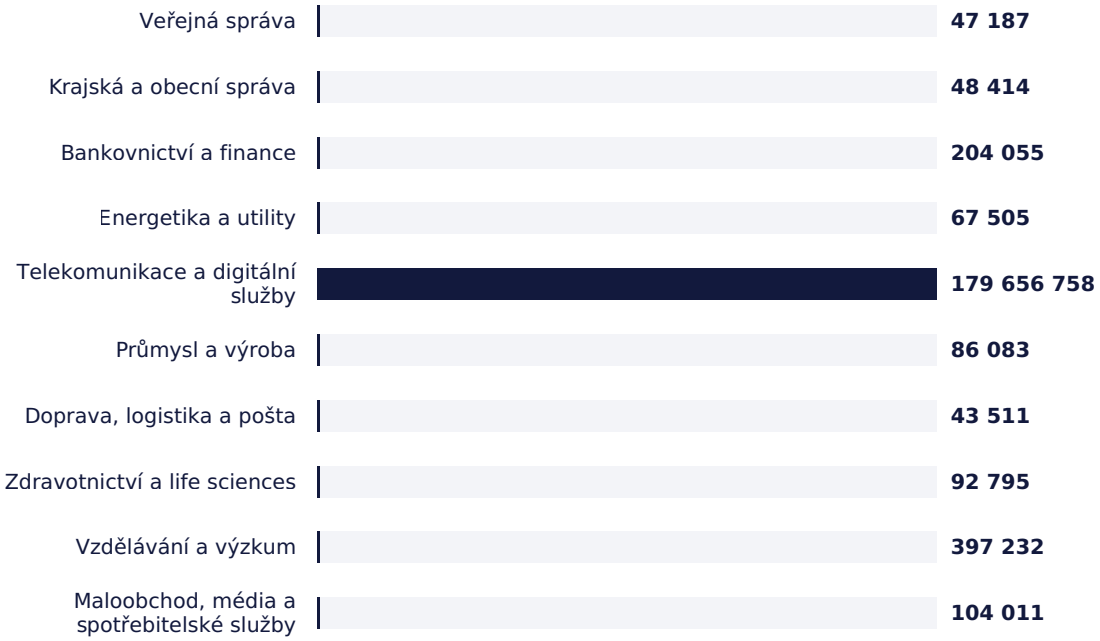
3.3 Vazby na infikovaná zařízení a historické záznamy hesel

Napříč všemi **250 hodnocenými českými doménami** vykázalo **221 domén (88,4 %) nejméně 318 706 vazeb na zařízení**, rozdělených na **24 224 zařízení označených jako zaměstnanecká** (u **168 domén**) a **294 482 nezaměstnaneckých zařízení** [S4]. Samostatně nashromáždilo **231 domén (92,4 %)** celkem **180 747 551 historických záznamů přihlašovacích údajů**: **86 659 575** z databází úniků, **9 161 620** z infostealerů a **84 926 356** z combolistů [S4].

Vazby na zařízení a historické záznamy hesel se koncentrují v telekomunikacích, maloobchodu, bankovnictví a vzdělávání



Historické záznamy přihlašovacích údajů (samostatné měřítko; Telekomunikace tvoří 99,4 %)



Zdroj: pozorování expozice Brandefense pro všech 250 hodnocených českých domén, snímek k 27. listopadu 2026 [S4]. Kumulativní vazby se mohou překrývat; nepředstavují unikátní osoby ani potvrzené průniky.

Sektorová skupina (po 25 hodnocených)	Vazby na zařízení (nejméně)	Zaměstnanecká zařízení	Ostatní zařízení	Záznamy hesel celkem	Databáze úniků	Infostealery	Combolisty	Vystavené dokumenty	30d podobné názvy
Veřejná správa	1 576	21	1 555	47 187	12 229	1 049	33 909	11	3 614
Krajská a obecní správa	720	46	674	48 414	26 177	2 115	20 122	16	22 073
Bankovnictví a finance	39 079	299	38 780	204 055	130 196	6 224	67 635	34	3 821
Energetika a utility	15 326	112	15 214	67 505	39 192	1 755	26 558	6	6 178
Telekomunikace a digitální služby	101 226	20 331	80 895	179 656 758	86 204 733	9 056 551	84 395 474	765	12 504
Průmysl a výroba	1 715	108	1 607	86 083	53 588	3 091	29 404	11	4 679

Sektorová skupina (po 25 hodnocených)	Vazby na zařízení (nejméně)	Zaměstnanecká zařízení	Ostatní zařízení	Záznamy hesel celkem	Databáze úniků	Infostealery	Combolisty	Vystavené dokumenty	30d podobné názvy
Doprava, logistika a pošta	14 375	152	14 223	43 511	16 173	3 918	23 420	10	11 751
Zdravotnictví a life sciences	7 361	153	7 208	92 795	49 064	4 193	39 538	10	98
Vzdělávání a výzkum	17 235	2 748	14 487	397 232	85 145	73 664	238 423	94	721
Maloobchod, média a spotřebitelské služby	120 093	254	119 839	104 011	43 078	9 060	51 873	53	2 806
Celkem (250 hodnocených)	**318 706**	**24 224**	**294 482**	**180 747 551**	**86 659 575**	**9 161 620**	**84 926 356**	**1 010**	**68 245**

Tři strukturální vzorce tato čísla vysvětlují a řídí třídění obránců [S4]:

- **Soustředění spotřebitelských webmailů vysvětluje 99,4 % historických hesel.** Telekomunikace a digitální služby představují **179 656 758** ze **180 747 551** záznamů hesel (**99,4 %**) [S4]. Dominantní české webmaily hromadí desetiletí opakovaně použitých hesel z cizích úniků bez důkazu průniku na servery operátora [S4]. Bez telekomunikací drží ostatních devět sektorů dohromady **1 090 793** historických záznamů, v čele se **Vzděláváním (397 232)**, **Bankovnictvím (204 055)** a **Maloobchodem (104 011)** [S4].
- **V maloobchodu a bankovnictví převažují klientská zařízení, ve vzdělávání zaměstnanecká.** Maloobchod drží **120 093** zařízení (**119 839** ostatních oproti **254** zaměstnaneckým) a Bankovnictví **39 079** (**38 780** ostatních oproti **299** zaměstnaneckým) [S4]. **Vzdělávání a výzkum** naproti tomu vykazuje **2 748 zařízení označených jako zaměstnanecká** u **24 z 25** domén [S4]. U spotřebitelských webmailů v telekomunikacích (`20 331` zařízení označených jako zaměstnanecká) mohou mnohé vazby patřit soukromým uživatelům, nikoli zaměstnancům; před zásahem je porovnejte s interní evidencí stanic [S4].
- **Kumulativní záznamy nejsou počty průniků roku 2026.** Historická hesla a zařízení sčítají víceleté záznamy překrývajících se osob a domén [S4]. Obránci nikdy nesmějí klást kumulativní expozici na roveň incidentům roku 2026 [S4].

3.4 Dokumenty, podobné domény a 365denní zmínky v podsvětí

Nad rámec hesel a zařízení vykázalo **101 z 250 domén** celkem **1 010 vystavených vazeb na dokumenty** (v čele s Telekomunikacemi **765**, Vzděláváním **94**, Maloobchodem **53** a Bankovnictvím **34**) [S4]. Samostatně vykazovalo **201 domén** celkem **68 245 pozorování podobných názvů za 30 dní** [S4]. Vysoké počty vykazuje **Krajská a obecní správa (22 073)**, **Telekomunikace (12 504)** a **Doprava (11 751)** [S4]. Krátké názvy obcí či obecných značek často připomínají cizí domény, takže každý nález vyžaduje kontrolu phishingového záměru [S4].

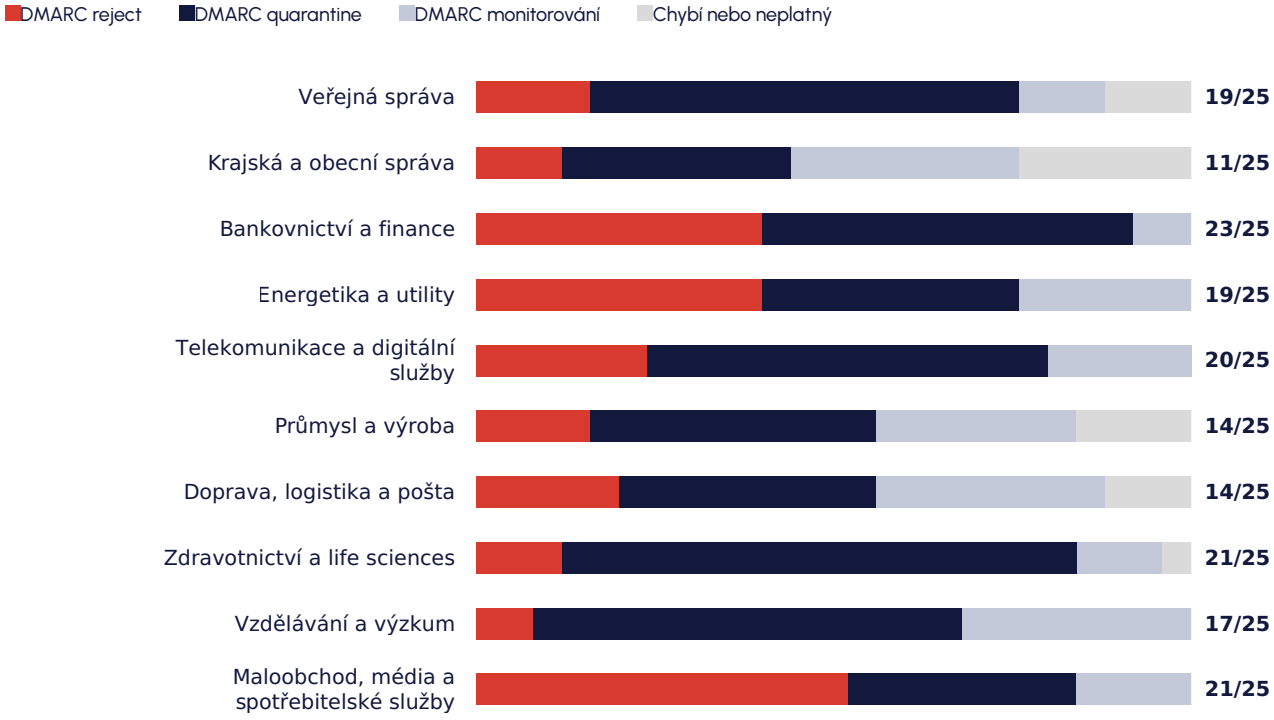
V klouzavém 365denním okně (**27. listopadu 2025 až 26. listopadu 2026**) mělo **33 z 250 domén (13,2 %)** celkem **1 931 zmínek v dark chatech** [S4]. Na dark webu mělo **16 domén (6,4 %)** celkem **230 zmínek** [S4]. V okně roku 2026 (**1. ledna až 26. listopadu 2026**) vygenerovalo **23 domén (9,2 %)** celkem **1 334 zmínek domén** [S4].

Telekomunikace a digitální služby soustředily **1 785 z 1 931 zmínek v dark chatech (92,4 %)** a **193 z 230 na dark webu (83,9 %)** [S4]. V roce 2026 na ně připadlo **1 291 z 1 334 zmínek (96,8 %)**, především na doménách spotřebitelských webmailů a digitálních služeb [S4]. Maloobchod zaznamenal **108 zmínek v dark chatech**, zatímco **Energetika** měla nulu a **Bankovnictví** jen **2 domény (3 zmínky v dark chatech, 0 na dark webu)** [S4].

3.5 Autentizace pošty, DNSSEC, TLS a HSTS u 250 českých domén

Pasivní kontrola z **27. listopadu 2026** ukazuje poměrně vyspělou českou základnu v kryptografickém podepisování DNS a autentizaci odesílatelů, avšak s výraznými sektorovými rozdíly u obecního a průmyslového DMARC [S3]. Z celkových 250 domén publikuje **179 (71,6 %)** politiku DMARC žádající `quarantine` (**119**) nebo `reject` (**60**), **54 (21,6 %)** zůstává v monitorovacím režimu (`p=none`) a **17 (6,8 %)** postrádá platný záznam DMARC [S3][S70].

Bankovnictví a maloobchod vedou ve vynucování DMARC, zatímco krajská a obecní správa výrazně zaostává



Hodnoty vpravo ukazují vynucující politiky (reject nebo quarantine) / 25 vybraných domén v sektoru. Zdroj: pasivní pozorování konfigurace 250 vybraných českých domén, snímek k 27. listopadu 2026 [S3]. Publikované politiky samy o sobě neprokazují vynucení na úrovni zpráv ani zabránění podvržení.

Podpůrné poštovní, DNS a transportní prvky ukazují stejně názorné silné stránky i mezery v 250doménovém snímku [S3]:

Sektorová skupina (po 25 doménách)	DMARC reject	DMARC quarantine	DMARC none	DMARC chybí / neplatný	DNSSEC DS	SPF přítomen	DKIM nalezen	CAA přítomen	HSTS nastaveno
Veřejná správa	4	15	3	3	25	24	18	17	22
Krajská a obecní správa	3	8	8	6	18	23	14	3	16
Bankovnictví a finance	10	13	2	0	20	25	20	9	21
Energetika a utility	10	9	6	0	20	25	20	4	16

Sektorová skupina (po 25 doménách)	DMARC p=reject	DMARC p=quarantine	DMARC p=none	DMARC chybí / neplatný	DNSSEC DS	SPF přítomen	DKIM nalezen	CAA přítomen	HSTS nastaveno
Telekomunikace a digitální služby	6	14	5	0	16	23	21	8	20
Průmysl a výroba	4	10	7	4	11	24	18	2	15
Doprava, logistika a pošta	5	9	8	3	13	25	18	3	15
Zdravotnictví a life sciences	3	18	3	1	19	25	20	7	10
Vzdělávání a výzkum	2	15	8	0	18	25	20	11	17
Maloobchod, média a spotřebitelské služby	13	8	4	0	13	25	22	4	11
Celkem (250 domén)	**60**	**119**	**54**	**17**	**173**	**244**	**191**	**68**	**163**

Pět technických zjištění zasluhuje přímou návaznou akci správců [S3]:

- **Mimořádně silné nasazení DNSSEC vedené ústřední správou.** Kultura domény `.cz` se projevuje zřetelně: **173 z 250 domén (69,2 %)** publikuje záznamy DNSSEC DS [S3]. Nasazení dosahuje **25 z 25 (100 %)** ve veřejné správě a **20 z 25 (80 %)** v bankovnictví i energetice [S3]. Průmysl a výroba (**11/25**) a doprava (**13/25**) zaostávají nejvíce [S3].
- **Krajská a obecní správa představuje nejširší mezeru v DMARC.** Pouze **11 z 25 (44 %)** krajských a obecních domén vynucuje DMARC (`3 reject` , `8 quarantine`) [S3]. Osm zůstává na `none` a **6** postrádá platnou politiku DMARC [S3]. Spolu se **14 z 25** vynucujícími doménami v průmyslu (4 chybějící) a **14 z 25** v dopravě (3 chybějící) zůstává **71 z 250 domén (28,4 %)** otevřeno přímému podvržení odesílatele [S3][S70].
- **Vysoká přítomnost SPF a DKIM usnadňuje přechod na přísnější DMARC.** Již **244 z 250 domén (97,6 %)** publikuje SPF a u **191 (76,4 %)** byl nalezen záznam DKIM [S3][S71][S72]. Většina z 54 monitorovacích domén tak může po vyhodnocení reportů přejít na `quarantine` nebo `reject` [S3][S70]. Samotná publikovaná značka DMARC podle RFC 7489 ještě nezaručuje stoprocentní pokrytí (`pct=100`) ani chování příjemce [S70].

- **Stav TLS, HSTS a CAA na dostupných koncových bodech.** Z 250 domén předložilo **238** platný certifikát TLS, **4** neprošly validací TLS a **8** nebylo možné k datu snímku posoudit [S3]. Z **227** dosažitelných HTTP koncových bodů (23 nedostupných) nastavilo **163 (71,8 % dosažitelných)** hlavičku HSTS [S3][S73]. Veřejná správa (22) a bankovnictví (21) vedly, zatímco zdravotnictví (10) a maloobchod (11) zaostávaly [S3]. Omezení certifikačních autorit CAA bylo přítomno u **68 z 250 domén (27,2 %)** [S3].
- **Rozmanitost poštovních serverů klade důraz na lokální záplatování.** Směrování pošty se dělilo mezi **88 domén (35,2 %)** na Microsoft 365 MX, **14** na Google Workspace a **4** bez MX záznamu [S3]. Zbývajících **144 domén (57,6 %)** provozuje domácí, evropské nebo vlastní poštovní servery [S3]. Záplatování vlastních serverů (například Zimbra `CVE-2025-66376`) proto zůstává v Česku stejně důležité jako obrana cloudového M365 [S3] [S8][S83].

3.6 Převod signálů expozice do oddělených ověřovacích front

Obránci by měli tato zjištění směrovat do tří samostatných provozních front místo jejich sloučení do jediného proudu výstrah:

1. **Fronta aktuálních nabídek přístupů (do 5 pracovních dnů).** Ověřte **66 domén** s aktivními nabídkami proti živým záznamům přihlášení, při shodě zrušte relace a zaznamenejte uzavření [S4].
2. **Rozdělená fronta třídění zařízení (30 dní).** Srovnejte zařízení označená jako zaměstnanecká (`24 224` u `168` domén) s evidencí firemních stanic a ponechte nezaměstnanecká zařízení (`294 482`) ve frontě klientských podvodů [S4].
3. **Fronta posílení pošty a DNS (30 dní).** Prověřte **71 domén** bez vynucujícího DMARC (prioritně obce, průmysl a dopravu) [S3][S70]. Opravte **4 neplatné certifikáty TLS** a zapněte HSTS a CAA na veřejných portálech [S3] [S73].

KLÍČOVÉ ZÁVĚRY

01

Napříč všemi 250 hodnocenými českými doménami k 27. listopadu 2026 činí národní souhrnná hodnota Atlas 48/100, přičemž 66 vykazuje aktuální nabídky přístupů a 221 nejméně 318 706 vazeb na zařízení.

02

Webmaily v telekomunikacích drží 99,4 % ze 180,7 mil. historických záznamů hesel, zatímco krajská a obecní správa má nejširší mezeru v DMARC (11 z 25, 6 chybí).

03

Prověřte aktuální nabídky do pěti pracovních dnů, oddělte firemní zařízení od klientských a přesuňte 71 domén na DMARC quarantine nebo reject.

KAPITOLA 04

Tvrzení a případy z podsvětí

TATO KAPITOLA ODPOVÍDÁ

Co aktéři kolem Česka skutečně nabízejí, poptávají a recyklují?

7

zdokumentovaných případů tvrzení z podsvětí na 16 doslovných kartách příspěvků

4.1 Jak číst tvrzení z podsvětí 29

4.2 Prodeje databází, recyklované úniky a nadsazená tvrzení 29

4.3 Zprostředkovatelé přístupů, chybně označené combolisty a nástroje na webmail 33

4.4 Telekomunikační obchvaty, padělané KYC doklady a poptávka po české silné identitě 37

KAPITOLA 04

Tvrzení a případy z podsvětí

VE ZKRATCE

Zaznamenané příspěvky z podsvětí ukazují aktivní trh kolem českých dat, přihlašovacích údajů, telekomunikačních obchvatů, padělaných KYC dokladů a účtů Bank iD či bílých koňů. Forenzní srovnání však ukazuje silnou recyklaci: inzerát e-shopu „Year: 2026 Fresh" z 22. listopadu odpovídá únorovému schématu z listopadu 2025. Údajný český soubor 121K pak ukazuje na `argentina.txt`. Každé tvrzení ověřte proti živým schématům dříve, než spustíte incidentní eskalaci.

4.1 Jak číst tvrzení z podsvětí

Inzerát v podsvětí dokládá jedinou ověřenou skutečnost: aktér k danému datu zveřejnil nabídku nebo poptávku [S1]. **Neprokazuje**, že byla česká organizace napadena, že jsou data čerstvá ani že došlo k obchodu [S1]. Z důvodu ochrany neověřených cílů a zamezení šíření vyděračských tvrzení jsou všechny nepotvrzené názvy firem, domény, přesné lokality a přezdívky autorů v případech A až G a na kartách `B01` až `B16` vynechány.

4.2 Prodeje databází, recyklované úniky a nadsazená tvrzení

A

PŘÍPAD A

Údajný export českého operátora a důkaz recyklace databáze e-shopu

Tvrzení neověřeno

Telekomunikace, e-commerce a portály

Klíčové ponaučení

Před vydáním oznámení o úniku ověřte inzerovanou strukturu tabulek a časová razítka proti živým exportům a starším archivům.

Karta důkazu B01 — 18. 2. 2026

Autor na fóru (přezdívka skryta) | Fórum | Fórum | Angličtina

ORIGINÁL

Offering a dataset originating from [Czech telecommunications provider]. It provides a detailed look at the organization's operations, including Contacts, Booking History, Customer Identity Verifications. The data is fresh and organized across 3 main sections.

PŘEKLAD

Nabízím datovou sadu pocházející od [český telekomunikační operátor]. Poskytuje detailní pohled na provoz organizace včetně tabulek Contacts, Booking History a Customer Identity Verifications. Data jsou čerstvá a rozdělená do 3 hlavních částí.

Poznámka. Název operátora je skryt, protože nebylo zjištěno žádné oficiální potvrzení úniku.

Doloženo
Prodejce na fóru používá opakující se třídílnou šablonu k nabídce údajných tabulek kontaktů, objednávek a ověření identity připisovaných českému telekomunikačnímu operátorovi.

Neprokázáno
Pravost dat, čerstvost získání, průnik do serverů, počet dotčených záznamů ani uskutečněný prodej.

Karta důkazu B02 — 24. 2. 2026

Autor na fóru (přezdívka skryta) | Fórum | Fórum | Angličtina

ORIGINÁL

Today i leak [Czech online retailer] client database enjoy it 105K lines leaked [...] Sample: [customer names and emails withheld]; 2025-11-25 18:09:19

PŘEKLAD

Dnes zveřejňuji klientskou databázi [český e-shop], 105 tis. řádků [...] Ukázka: [jména a e-maily zákazníků skryty]; 2025-11-25 18:09:19

Poznámka. Jména zákazníků, e-maily i doména e-shopu jsou odstraněny; karta B13 nabízí stejnou strukturu o devět měsíců později jako čerstvou databázi z roku 2026.

Doloženo
Únorový příspěvek na fóru zveřejňuje údajnou databázi 105 000 řádků zákazníků českého e-shopu, jejíž ukázková časová razítka končí koncem listopadu 2025.

Neprokázáno
Datum původního průniku, celistvost souboru, platnost hesel ani oficiální potvrzení úniku.

Karta důkazu B13 — 22. 11. 2026

Autor na fóru (přezdívka skryta) | Fórum | Fórum | Angličtina

ORIGINÁL

A structured 2026 customer/business database associated with [Czech online retailer], containing approximately 105K records with customer, employee, sales, and account information. Country: Czech Republic Year: 2026 Data Status: Fresh Records: 105K+ [sample row withheld]

PŘEKLAD

Strukturovaná zákaznická a obchodní databáze z roku 2026 spojená s [český e-shop] obsahující přibližně 105 tis. záznamů o zákaznících, zaměstnancích, prodejích a účtech. Země: Česká republika Rok: 2026 Stav: Čerstvá Záznamy: 105 tis.+ [ukázkový řádek skryt]

Poznámka. Dva další inzeráty ze dne 22. listopadu na stejném fóru nárokovaly data nejmenovaného českého webového portálu (třítabulková šablona) a českého poskytovatele internetu; jeden z nich ponechal v textu automaticky generovanou poznámku o odvození struktury.

Doloženo
Dne 22. listopadu 2026 prodejce na fóru znovu inzeruje tutéž přibližně 105tisícovou strukturu českého e-shopu, která se poprvé objevila v únoru (B02), tentokrát jako čerstvou databázi z roku 2026.

Neprokázáno
Jakýkoli listopadový průnik z roku 2026, nově získaná zákaznická data ani oficiální potvrzení úniku.

Tři vlákna na fórech z února a listopadu 2026 ukazují strukturovaný marketing databází i systematické přepisování dat [S1]. Dne **18. února** zveřejnil prodejce třídílný export připisovaný českému telekomunikačnímu operátorovi (`B01`), rozdělený na zákaznické profily, objednávky a fakturaci [S1]. Dne **24. února** nabídlo jiné vlákno přibližně **105 000 řádků** údajné databáze českého e-shopu (`B02`), jejíž ukázkové schéma končilo časovými značkami **25. listopadu 2025** [S1].

O devět měsíců později, **22. listopadu 2026**, prodejce znovu inzeroval **přesně totéž schéma o ~105 000 řádcích** s nálepkou **„Year: 2026 Fresh"** (`B13`) [S1]. Téhož dne se objevila dvě další česká databázová vlákna [S1]. Jedno z nich v popisu omylem ponechalo šablonový text AI odhadu schématu [S1]. Žádný z dotčených subjektů nepotvrdil odpovídající únik roku 2026 a všechny nepotvrzené názvy firem zůstávají skryty [S1]. Pro české týmy SOC z případu A plyne jasné ověřovací pravidlo: archivujte názvy sloupců a nejnovější časové značky ze starších inzerátů, abyste recyklované „čerstvé" úniky rychle odhalili [S1].

PŘÍPAD B

B

Neověřené telegramové tvrzení o 6,5 milionu českých finančních kontaktů

Tvrzení neověřeno

Finanční a pojišťovací data

Klíčové ponaučení

Považujte neověřené telegramové nabídky milionových databází za nepotvrzené, dokud interní záznamy či vzorky neprokážou reálný původ.

Karta důkazu B03 — 29. 1. 2026

Autor v kanálu (přezdívka skryta) | Telegramový kanál | Telegram | Ruština

ORIGINÁL

Продается чешская база данных. 6.5 миллионов строк (3 банка, одна страховая компания). Не была в общем доступе. [...] В строке (номер телефона, ФИО, улица, дом, квартира, город, индекс). Продажа от 100т строк за раз.

PŘEKLAD

Na prodej česká databáze. 6,5 milionu řádků (3 banky, jedna pojišťovna). Nebyla veřejně dostupná. [...] Pole: telefon, celé jméno, ulice, číslo popisné, byt, město, PSČ. Prodej od 100 tis. řádků najednou.

Poznámka. Inzerát neuvádí názvy institucí ani ověřitelné vzorky; marketingová tvrzení o prvním zdroji neprokazují kompromitaci banky.

Doloženo
Ruskojazyčný inzerát na Telegramu nabízí údajnou českou kontaktní databázi o 6,5 milionu řádků připisovanou obecně třem bankám a jedné pojišťovně po balících 100 000 řádků.

Neprokázáno
Jakýkoli průnik do české banky či pojišťovny, správnost počtu řádků, unikátní osoby, čerstvost dat ani uskutečněný obchod.

Dne **29. ledna 2026** nabízel ruskojazyčný prodejce na Telegramu údajných **6,5 milionu českých spotřebitelských záznamů** (`B03`) [S1]. Inzerát je připisoval „3 bankám a 1 pojišťovně“ a nabízel po balících **100 000 řádků** [S1]. Žádná česká banka ani pojišťovna nepotvrdila odpovídající hromadný únik a inzerát neobsahoval ověřitelné interní identifikátory [S1]. Velká zaokrouhlená tvrzení na Telegramu cílená na Česko často spojují stažené marketingové katalogy, starší soubory nebo zahraniční tabulky přelepené domácími finančními štítky [S1]. Obránci by měli vyžadovat ověřitelná klientská pole existující výhradně v interních systémech, než začnou milionové nabídky pokládat za živý průnik [S1].

4.3 Zprostředkovatelé přístupů, chybně označené combolisty a nástroje na webmail

PŘÍPAD C

Zprostředkovatel počátečního přístupu nabízející údajné české finanční RDP

Nabídka neověřena

Přístup do finančních služeb

Klíčové ponaučení

Odstraňte přímé RDP z veřejného internetu, zaveďte vícefaktorové ověření odolné proti phishingu a prověřte privilegovaná přihlášení.

Karta důkazu B04 14. 4. 2026

Autor na fóru (přezdívka skryta) Fórum Fórum Angličtina

ORIGINÁL

500 new listings were added today [...] Some Financial Services Fresh Access for sale: [RDP] Financial Services - Czech Republic (Unknown revenue) | Type: RDP | Privilege: Root (Linux) | AV / EDR: Carbon Black

PŘEKLAD

Dnes přidáno 500 nových nabídek [...] Čerstvé přístupy ve finančních službách na prodej: [RDP] Finanční služby – Česká republika (neznámý obrat) | Typ: RDP | Oprávnění: Root (Linux) | AV / EDR: Carbon Black

Poznámka. Zveřejněno v dubnu, kdy NÚKIB evidoval poloviční podíl kategorie Průnik na všech českých incidentech.

Doloženo
Dubnový příspěvek na fóru inzeruje údajný přístup přes vzdálenou plochu (RDP) do nejmenovaného subjektu finančních služeb v Česku s označením bezpečnostního agenta.

Neprokázáno
Platnost aktivního přístupu, totožnost cíle, privilegovanou kompromitaci, vnitřní soulad technických štítků ani uskutečněný prodej.

Dne **14. dubna 2026** inzeroval zprostředkovatel počátečního přístupu na fóru nabídku `[RDP] Financial Services - Czech Republic` (`B04`) [S1]. Přestože samotný přístup zůstává neověřený a žádná česká finanční instituce nebyla jmenována ani potvrzena, záznam dokládá trvalou poptávku po vystavených rozhraních Remote Desktop Protocol ve středoevropských finančních firmách [S1]. IT týmy ve financích a poradenství by měly odstranit přímé RDP z veřejného internetu, vynutit MFA odolné proti phishingu na branách vzdáleného přístupu a prověřit podezřelá vzdálená přihlášení [S1].

PŘÍPAD D

D

Chybně označené zahraniční combolisty, výpisy infostealerů a kontrolory českých webmailů

Spotřebitelské e-maily a portály

Tvrzení neověřeno

Klíčové ponaučení

Berte seznamy hesel vázané na URL jako pravděpodobnou krádež ze zařízení uživatelů, prověřujte původ souborů a blokujte credential stuffing.

Karta důkazu B05 — 24. 1. 2026

Autor na fóru (přezdívka skryta) | Fórum | Fórum | Angličtina

ORIGINÁL

Database: Czech Republic Type: Email : Password Date: [24/JAN/2026] Combo: [121 K++] Line Status: FRESH | HQ [...] [file-host link ending in]/argentina.txt

PŘEKLAD

Databáze: Česká republika Typ: E-mail : Heslo Datum: [24/JAN/2026] Combo: [121 tis.++] Stav: FRESH | HQ [...] [odkaz končící]/argentina.txt

Poznámka. Odkazy na úložiště a kontakty jsou odstraněny; nesoulad názvu souboru dokládá běžné přeznačování recyklovaných mezinárodních seznamů podle zemí.

Doloženo
Lednový příspěvek na fóru propaguje údajný čerstvý český seznam 121 000 e-mailů a hesel, jehož vlastní zrcadlový odkaz nese název souboru argentina.txt.

Neprokázáno
Český původ záznamů, funkční hesla, čerstvou kompromitaci z roku 2026 ani původ z jediné organizace.

Karta důkazu B06 — 15. 5. 2026

Autor na fóru (přezdívka skryta) | Fórum | Fórum | Angličtina

ORIGINÁL

[Czech telecommunications portal] Logs (100 Lines) [...] Total Lines: 100 Content Type: URL / Email / Password Combo Date Uploaded: 2026-05-15 [sample login strings withheld]

PŘEKLAD

Logy [český telekomunikační portál] (100 řádků) [...] Celkem řádků: 100 Typ obsahu: URL / E-mail / Heslo Datum nahrání: 2026-05-15 [ukázky přihlášení skryty]

Poznámka. Výpisy filtrované podle URL obvykle odrážejí krádež přihlašovacích údajů z infikovaných zařízení koncových uživatelů, nikoli kompromitaci dané služby.

Doloženo
Květnový příspěvek šíří 100 řádků URL, uživatelských jmen a hesel vyfiltrovaných pro zákaznický portál českého telekomunikačního operátora (týž den doplněný obdobným 100řádkovým výpisem pro českou streamovací službu).

Neprokázáno
Serverový průnik u kteréhokoli z obou českých poskytovatelů, aktuální platnost hesel ani převzetí účtů.

Karta důkazu B07 2. 3. 2026

Autor na fóru (přezdívka skryta) Fórum Fórum Angličtina

ORIGINÁL

17K GOOD COMBO DATABASE (.cz) DOWNLOAD [file-host link withheld]

PŘEKLAD

17 tis. dobrá combo databáze (.cz) ke stažení [odkaz na úložiště skryt]

Poznámka. Odkazy ke stažení jsou odstraněny; opakované menší balíčky slouží k testování opakovaně používaných hesel na českých webmailech i firemních doménách.

Doloženo
Březnový příspěvek na fóru šíří seznam 17 000 přihlašovacích párů označených pro domény .cz, vedle opakovaných měsíčních balíčků po 1 000 řádcích českých e-mailových přístupů od února do října.

Neprokázáno
Aktivní přístup do schránek, unikátní osoby, čerstvé získání ani průnik do konkrétní instituce.

Karta důkazu B14 19. 11. 2026

Autor na fóru (přezdívka skryta) Fórum Fórum Angličtina

ORIGINÁL

1.5K Czech Acccess Just HQ Mail 19.11 [paste-host link withheld]

PŘEKLAD

1,5 tis. českých e-mailových přístupů 19.11 [odkaz na úložiště skryt]

Poznámka. Odkazy na úložiště jsou odstraněny; ilustruje trvalou nabídku pro útoky credential stuffing v nedávném okně 12.–26. listopadu.

Doloženo
Příspěvek z 19. listopadu sdílený na dvou fórech distribuuje 1 500 řádků českých e-mailových přístupů, vedle listopadových inzerátů hromadného ověřovače IMAP/POP3/SMTP podporujícího české spotřebitelské webmailové služby.

Neprokázáno
Funkční přihlašovací údaje, unikátní české uživatele, kompromitaci serverů poskytovatele pošty ani čerstvé získání.

Čtyři nálezy na fórech z ledna, března, května a listopadu 2026 ukazují, proč surové seznamy hesel jen zřídka znamenají průnik na české servery [S1]. Dne **24. ledna** inzeroval autor `121K++ Czech Republic` přihlašovací údaje (`B05`), ale vlastní odkaz ke stažení mířil přímo na soubor `argentina.txt`, což dokládá prosté geografické přeznačení [S1]. Dne **2. března** nahrál prodejce `17K (.cz)` e-mailů a hesel spolu s opakovanými měsíčními balíky `1K` (`B07`) [S1].

Dne **15. května** sdílel autor stořádkové výpisy filtrované podle URL označené pro české telekomunikační a streamovací portály (`B06`), typický znak záznamů infostealerů z koncových zařízení spíše než průniků do databází operátorů [S1]. V nedávném období **19. listopadu** nabídlo jiné vlákno `1.5K Czech Mail Access` (`B14`) [S1]. V polovině listopadu navíc marketing nástrojů propagoval automatizovaný kontrolor `Krantz Mail` výslovně podporující české spotřebitelské webmailové služby [S1]. Spotřebitelské platformy by měly na výpisy podle URL a kontrolory reagovat přísným omezením pokusů o přihlášení, detekcí credential stuffingu a povinným MFA [S1].

4.4 Telekomunikační obchvaty, padělané KYC doklady a poptávka po české silné identitě

PŘÍPAD E

E

Trasy podvržení SMS a hovorů, IMSI catchery a pronájem českých SIM

Telekomunikace a SMS

Inzerované služby

Klíčové ponaučení

Opusťte ověřování přes SMS, ověřte u operátorů filtry proti spoofingu a varujte klienty, že úřady neposílají platební odkazy v SMS.

Karta důkazu B08 — 23. 7. 2026

Autor na fóru (přezdívka skryta) | Fórum | Fórum | Angličtina

ORIGINÁL

[service domain withheld] sms and call spoofing with 180 and more destinations. Majority of countries allow spoofing senderid [...] Shipping and selling IMSI catcher to all Europe and Ukraine [...] no limits, no kyc, only crypto.

PŘEKLAD

[doména služby skryta] podvrhování SMS a hovorů do více než 180 destinací. Většina zemí umožňuje podvržení odesílatele [...] Prodej a zasílání IMSI catcherů po celé Evropě a na Ukrajinu [...] bez limitů, bez KYC, pouze kryptoměny.

Poznámka. Samostatné červnové příspěvky na Telegramu inzerovaly české alfanumerické SMS trasy; ČTÚ již dříve upozornil na přesun podvodníků k SMS phishingu po zavedení filtrů hlasového spoofingu.

Doloženo

Červencový inzerát napříč několika fóry nabízí globální podvrhování SMS a telefonních čísel ve více než 180 zemích a evropské dodávky přenosných falešných základnových stanic za kryptoměny.

Neprokázáno

Skutečnou doručitelnost v českých mobilních sítích, ověřené dodání hardwaru ani vazbu na konkrétní českou podvodnou vlnu.

Karta důkazu B09 — 21. 11. 2026

Autor na fóru (přezdívka skryta) | Fórum | Fórum | Ruština

ORIGINÁL

Аренда физических SIM мобильных операторов для приёма SMS MNO и MVNO - только реальные SIM: мы не используем VoIP и виртуальные АТС. Для регистраций и долгосрочной работы с сервисами [...] 18+ countries [...] 30 дней - от $4.00

PŘEKLAD

Pronájem fyzických SIM karet mobilních operátorů pro příjem SMS (MNO a MVNO – pouze skutečné SIM, nepoužíváme VoIP ani virtuální ústředny). Pro registrace a dlouhodobou práci se službami [...] 18+ zemí [...] 30 dní od 4 USD.

Poznámka. Odkazy a kontakty služby jsou odstraněny; pronájem fyzických SIM se nabízí k obcházení blokace virtuálních čísel při online registracích.

Doloženo

Listopadový inzerát na fóru nabízí dlouhodobý pronájem fyzických ne-VoIP SIM linek pro příjem SMS ve více než 18 zemích včetně Česka a navazuje na únorové nabídky českých eSIM.

Neprokázáno

Zapojení českých operátorů, reálnou zásobu linek ani prokázané využití při konkrétním převzetí českých účtů.

Nabídka telekomunikačních nástrojů v podsvětí se v roce 2026 vyvíjela souběžně s českým tažením proti spoofingu [S1][S34][S35]. Dřívější vlákna nabízela české profily eSIM (`11. února`) a české alfanumerické SMS Sender ID trasy (`6. června`) [S1]. Dne **23. července** propagovaly inzeráty na více fórech **brány pro podvržení SMS a hovorů do více než 180 destinací** spolu s evropským hardwarem IMSI catcherů (`B08`) [S1].

V nedávném období **21. listopadu** inzerovalo ruskojazyčné vlákno pronájem **fyzických českých SIM karet** mimo VoIP (`SMS Arena`) pro příjem ověřovacích SMS kódů (`B09`) [S1]. Tyto nabídky přímo navazují na varování Českého telekomunikačního úřadu (ČTÚ), že blokování podvržených volání z pevných linek přesunulo podvodníky ke smishingu a zneužívání SMS ověřování [S34][S35].

PŘÍPAD F

F

Zakázkové padělky českých faktur a výplatních pásek, balíky EU KYC a nastrčené české firmy

Ověřování identity a firem

Inzerované služby

Klíčové ponaučení

Doplňte kontrolu nahraných dokladů o ověření v registrech, kontrolu živosti a zesílenou prověrku nově založených českých firem.

Vstupy pro podvody sahají daleko za kradená hesla až k padělaným českým dokumentům a hotovým schránkovým firmám, doloženým na kartách `B10` , `B11` a `B12` v §8.2 [S1]. Dne **21. srpna** nabízel prodejce na fóru **zakázkové české doklady o adrese, faktury za energie a výplatní pásky** (`B10`) [S1]. Dne **19. srpna** nabídl jiný prodejce **balíky EU KYC dokladů a selfie za 25 USD** včetně Česka (`B11`), v návaznosti na nábor z **19. dubna** platící **30 USD** za živé ověřovací odkazy [S1].

Dříve, **12. ledna**, inzerovalo ruskojazyčné vlákno **nastrčené české OSVČ za 3 500 USD** a **české s.r.o. za 4 900 USD** údajně včetně firemního účtu a hardwarového tokenu elektronického podpisu (`B12`) [S1]. Přestože úspěšnost založení zůstává neověřená, inzeráty ukazují snahu organizovaných podvodníků obejít české bankovní a AML kontroly už při zakládání účtů [S1].

PŘÍPAD G

G

Přímá poptávka po české Bank iD a MojeID a přeshraniční předávky legalizačních účtů

Bankovnictví, Bank iD a MojeID

Poptávka neověřena

Klíčové ponaučení

Přidejte dodatečné ověření při registraci přes Bank iD a MojeID, sledujte rychlé výběry z nových účtů a sdílejte varování mezi bankami.

Kapitoly 8 a 9 rozebírají bankovní dopady těchto vstupů na kartách `B15` a `B16` [S1]. Mezi **10. a 12. srpnem 2026** poptávali kupci na Telegramu **českou Bank iD za 100 USD za účet**, po dřívější poptávce ze 4. února [S1]. Zveřejnili také výzvu `WTB. KYC MojeID. Only Czech Republic` (`B15`) [S1].

Od ledna do října koordinovali ruskojazyční a ukrajinskojazyční zprostředkovatelé na Telegramu **předávky legalizačních bankovních účtů v Praze, Bratislavě, Varšavě a Vratislavi** (B16) [S1]. Inzeráty uváděly ceny **170 až 700 USD za retailový účet** nebo **provizi 20 % až 35 % z vybraných prostředků** (názvy bank začerněny) [S1]. Případy F a G dohromady propojují nabídku z podsvětí přímo s **legalizačními účty** sledovanými Policií ČR a s vlnou **11,8 miliardy Kč** bankovních podvodů evidovanou Českou bankovní asociací (ČBA) [S25][S29][S30][S31].

KLÍČOVÉ ZÁVĚRY

01

Forenzní srovnání inzerátu českého e-shopu „Year: 2026 Fresh" z 22. listopadu s vláknem z 24. února odhalilo přesnou recyklaci schématu z roku 2025.

02

Chybně označené zahraniční combolisty ([redacted]) a výpisy infostealerů vysvětlují většinu českých balíků hesel bez důkazu průniku na servery.

03

Pronájem fyzických českých SIM, padělané výplatní pásky, nastrčené s.r.o. a poptávka po Bank iD přímo napájejí domácí podvodné a legalizační sítě.

KAPITOLA 05

Veřejné incidenty, dodavatelé a nedávný vývoj

05

TATO KAPITOLA ODPOVÍDÁ

Které veřejně potvrzené incidenty zasáhly české organizace v roce 2026, včetně období 12. až 26. listopadu?

11

veřejných případových složek pokrývajících potvrzené české výpadky a úniky

5.1 Jaro až polovina léta 2026: obecní ransomware, routery a okrajové botnety 41

5.2 Srpen až začátek listopadu 2026: WordPress, finanční dcery, SaaS, PHP2Shell a OT varování 43

5.3 Nedávný vývoj: 12. až 26. listopadu 2026 45

KAPITOLA 05

Veřejné incidenty, dodavatelé a nedávný vývoj

VE ZKRATCE

Veřejně potvrzené české incidenty roku 2026 se soustředily kolem čtyř vektorů: obecního a obchodního ransomwaru, zranitelností webu a routerů, dodavatelů třetích stran a přístupu přes webovou aplikaci k univerzitní databázi. Zásadní případy zasáhly Jemnici, Židlochovice, Náměšť nad Oslavou, Šumperk, nebankovní části skupiny Partners, BitFakturu, Rohlík.cz, ČVUT, Univerzitu Karlovu, Dedoles a PRO-DOMA. Tři velké události nastaly mezi 12. a 26. listopadem odděleně od nekybernetického výpadku ministerstev. Záplatujte §12.2 a prověřte archivy dodavatelů ještě dnes.

5.1 Jaro až polovina léta 2026: obecní ransomware, routery a okrajové botnety

PŘÍPAD H

H

Jarní vlna kyberútoků na obce v Jemnici, Židlochovicích a Náměšti nad Oslavou

Potvrzené útoky

Místní a obecní samospráva

Klíčové ponaučení

Udržujte testované offline zálohy pro kompletní obnovu úřadu a přesuňte domény samospráv z pasivního či chybějícího DMARC.

Tři moravské a vysočinské obce zasáhly během několika jarních týdnů 2026 rušivé kyberútoky, které ukázaly, jak malé obecní IT týmy zvládají ransomware [S37][S38][S39][S40]. Dne **9. března** zasáhl ransomware **Městský úřad Jemnice**, narušil úřední systémy a vynutil si postupné obnovování služeb pro občany; Ransompedia později 6. dubna zaznamenala odpovídající položku **Lockbit5** [S2][S37].

O necelý týden později, **15. března**, zašifroval ransomware **Deadlock** systémy **Městského úřadu Židlochovice** [S38][S39]. Celostátní reportáž o měsíc později popsala dlouhou obnovu zahrnující hotovostní platby na přepážkách a papírovou agendu během znovuvybudování IT [S39]. Ransompedia zaznamenala odpovídající záznam **Deadlock** dne **10. července**, přičemž radnici chybně zařadila do sektoru `medias-and-audiovisual` [S2]. Ve stejném období koncem března a začátkem dubna zasáhl kyberútok **Městský úřad Náměšť nad Oslavou**, kde správci čistě obnovili zhruba **70 pracovních stanic** z **offline záloh** [S40].

PŘÍPAD I

Botnet REDHEBERG VNC a zásah Vojenského zpravodajství proti APT28 u routerů TP-Link

Oficiální varování

Vystavené VNC a SOHO routery

Klíčové ponaučení

Okamžitě odpojte neověřené služby VNC z veřejného internetu a nahraďte nebo izolujte nepodporované routery TP-Link.

Dvě oficiální jarní varování zdůraznila riziko vystavených domácích, malopodnikových a nespravovaných okrajových zařízení v Česku [S6][S7][S61][S62][S84]. Ve svém přehledu za Q1 2026 uvedl NÚKIB více než **3 200 českých zařízení** zapojených do botnetu **REDHEBERG** prostřednictvím internetově dostupných služeb Virtual Network Computing (VNC) [S6].

V dubnu 2026 zdokumentovaly FBI IC3 (`PSA260407`) a čtvrtletní přehled NÚKIB za Q2 rozsáhlé zneužívání starších **SOHO routerů TP-Link** (`CVE-2023-50224`), které citované agentury připsaly ruské vojenské rozvědce (**GRU / APT28**) [S7][S61][S62][S84]. NÚKIB uvedl, že **Vojenské zpravodajství** provedlo **aktivní obranný zásah** k ochraně zasažených českých routerů [S7]. Protože starší modely TP-Link, jako je vyřazený `TL-WR841N`, již nedostávají běžné záplaty, jedinou trvalou obranou zůstává výměna za podporovaný hardware a vypnutí vzdálené správy z internetu (§12.2) [S62][S84].

PŘÍPAD J

Červencový kyberútok na Městský úřad Šumperk a městskou policii

Potvrzený průnik

Městská správa

Klíčové ponaučení

Oddělte sítě městského úřadu a městské policie, připravte nouzový režim pokladen a včas hlaste incidenty úřadům.

Koncem **července 2026** zasáhl kyberútok **Městský úřad Šumperk** a současně narušil IT systémy **městské policie** [S41]. Policie ČR zahájila trestní vyšetřování [S41]. Dne **28. září** zveřejnila vyděračská skupina **Safepay** odpovídající záznam na Ransompedia, přičemž radnici chybně zařadila pod `retail-and-commerce` [S2]. Případ Šumperka ukazuje, proč musejí být sítě městské policie přísně odděleny od obecného kancelářského IT radnice [S41].

5.2 Srpen až začátek listopadu 2026: WordPress, finanční dcery, SaaS, PHP2Shell a OT varování

PŘÍPAD K

K

Vlna zneužívání WordPress wp2shell a malware ClickFix / PSW.Agent

Potvrzené zneužití

Veřejné weby a koncové stanice

Klíčové ponaučení

Okamžitě aktualizujte jádro WordPressu kvůli chybám wp2shell a omezte spouštění vložených příkazů používaných v útocích ClickFix.

V **srpnu 2026** udeřilo hromadné zneužívání dvou zřetězených chyb jádra WordPressu známých jako `wp2shell` [S63][S77][S78]. Spojují záměnu směrování dávkového REST API (`CVE-2026-63030` , CVSS 9,8) s SQL injekcí v parametru `author__not_in` třídy `WP_Query` (`CVE-2026-60137` , CVSS 5,9) [S77][S78]. Srpnový a Q3 přehled NÚKIB spojily tuto vlnu s **osmi revidovanými významnými českými incidenty** (původně devíti) [S8][S15]. Obě CVE figurují v katalogu CISA KEV a posunuly kategorii Průnik zhruba na dvě třetiny všech incidentů NÚKIB ve třetím čtvrtletí [S8][S77][S78].

Souběžně na koncových stanicích označila telemetrie ESET Česko za Q3 2026 techniku **ClickFix** za hlavní cestu šíření infostealerů `PSW.Agent` na počítačích macOS v Česku [S60]. Tyto návnady navádějí uživatele ke zkopírování a spuštění škodlivých příkazů z falešných ověřovacích stránek [S60]. Webové týmy musejí udržovat WordPress na verzích `6.8.6+` , `6.9.5+` nebo `7.0.2+` (§12.2), zatímco správci koncových stanic by měli omezit spouštění skriptů a školit personál proti příkazům copy-paste [S60][S63][S77][S78].

PŘÍPAD L

L

Únik v nebankovních dcerách skupiny Partners a oddělení bankovní infrastruktury

Potvrzený únik

Finanční poradenství a pojišťovnictví

Klíčové ponaučení

Oddělte licencované bankovní systémy od nebankovní IT infrastruktury skupiny a varujte klienty před navazujícím podvodným kontaktováním.

Dne **23. srpna 2026** (veřejně oznámeno **27. srpna**) zasáhl kyberútok čtyři nebankovní finanční a pojišťovací společnosti české skupiny **Partners** [S42][S43]. Průnik zpřístupnil osobní údaje klientů společností **Partners Financial Services**, **Simplea**, **Rentea** a **Partners investiční společnost** [S42][S43]. Zásadní bylo oficiální oznámení **Partners Banky**, že její samostatná regulovaná bankovní infrastruktura a klientské účty **nebyly incidentem zasaženy** [S42].

Dne **16. září** a znovu **12. listopadu** zveřejnila skupina **INC Ransom** položku `Partners Financial Services, a.s.` na svém únikovém webu, což tvoří jeden ze dvou opakovaných českých záznamů Ransompedia roku 2026 [S2]. Partners Banka uvedla, že její samostatná bankovní infrastruktura zasažena nebyla [S42]. Oddělení licencovaných bankovních systémů a identit od přidružených dcer omezuje cesty, kudy se útočník může šířit.

PŘÍPAD M

M

Průnik do fakturační databáze BitFaktura v Polsku a Česku

Cloudové fakturační služby

Potvrzený únik

Klíčové ponaučení

Vyměňte ohrožené API klíče, omezte integrace na povolené IP adresy a každou změnu bankovního účtu dodavatele ověřte zpětným telefonátem.

Mezi **27. a 28. zářím 2026** měl útočník přibližně **38 hodin** neoprávněný přístup do databáze online fakturační služby **BitFaktura** (`bitfaktura.cz`), což zasáhlo **všechny účty** v Polsku a Česku [S44][S45]. Oznámení společnosti z **29. září až 6. října** potvrdila, že údaje o platebních kartách v zasažené databázi uloženy nebyly [S44]. Provozovatel informoval **CERT Polska**, polský úřad pro ochranu údajů (**UODO**) a český **ÚOOÚ** [S44][S45]. Protože fakturační databáze obsahují seznamy dodavatelů, daňová čísla a čísla účtů IBAN tisíců malých firem, měly by české podniky varovat účetní před podvody se změněným číslem účtu na faktuře [S44][S45].

PŘÍPAD N

N

Únik z nástroje zákaznické podpory Rohlík.cz

Online prodej potravin

Potvrzený únik

Klíčové ponaučení

Omezte přístupy a dobu uchovávání dat v nástrojích zákaznické podpory i AI asistentů a varujte zákazníky před cílenými podvody.

Dne **11. října 2026** oznámil velký český online supermarket **Rohlík.cz** neoprávněný přístup do **nástroje zákaznické podpory**, který odhalil chaty, přepisy hovorů a e-maily zákazníků z období **duben až říjen 2026** [S46][S47]. Společnost potvrdila, že **hesla ani platební karty nebyly dotčeny**, a událost nahlásila **ÚOOÚ** i **NÚKIB** [S46][S47]. I bez hesel či karet poskytuje šest měsíců skutečných reklamací a objednávek podvodníkům vysoce věrohodné záminky pro cílený smishing a telefonické podvody [S46][S47].

PŘÍPAD O

Říjnová vlna PHP2Shell u Úřadu vlády ČR, ČHMÚ a ČVUT

Vládní weby a vysoké školy

Odstávka a útok

Klíčové ponaučení

Předem schvalte rychlé preventivní odstavení webů před vydáním oprav a aktualizujte PHP na aktuální listopadová bezpečnostní vydání.

Dne **21. října 2026** byly zveřejněny dvě kritické chyby vzdáleného spuštění kódu v PHP nazvané **PHP2Shell** (`CVE-2026-109618` , CVSS 9,8, a `CVE-2026-109619` , CVSS 8,1) [S74][S75]. Okamžitě vyvolaly narušení provozu českých veřejných a akademických webových portálů [S17][S48][S50]. Po mimořádném varování NÚKIB provedl **Úřad vlády ČR** zhruba **dvouhodinovou preventivní odstávku webu** bez potvrzeného průniku, zatímco **Český hydrometeorologický ústav (ČHMÚ)** omezil dotčené online služby [S48][S50].

Na **Českém vysokém učení technickém v Praze (ČVUT)** obránci zastavili **aktivní pokus o zneužití** a přistoupili k částečnému odstavení systémů [S49]. O měsíc později, **19. listopadu**, oznámil projekt PHP samostatnou kritickou chybu neshody serializace relací (`CVE-2026-115560` / `GHSA-658j-r8rw-q6mx` , CVSS 4.0 skóre 9,2) [S65][S76]. **Listopadová vydání z 19. listopadu** (`8.5.13` , `8.4.28` , `8.3.37` , `8.2.36` či novější) proto představují povinnou aktuální úroveň nápravy (§12.2) [S64][S65].

Samostatně zasáhla začátkem listopadu evropská vlna kyberútoků internetově dostupné **řídicí jednotky chlazení v obchodech** [S51]. Dne **11. listopadu** vydal NÚKIB preventivní varování vyzývající české provozovatele k oddělení průmyslového chlazení a automatizace budov od veřejného internetu, přičemž do uzávěrky nebyla v Česku potvrzena žádná oběť [S51]. Obdobně globální zneužívání nultých dnů **Citrix NetScaler ADC a Gateway** (`CVE-2026-88771` , `CVE-2026-88772` , doplněné 12. listopadu o `CTX697305` / `CVE-2026-120868`) nemělo do uzávěrky veřejně jmenovanou českou oběť [S79][S80][S81]. Obě oblasti zůstávají naléhavou prioritou záplatování v §12.2 [S79][S80][S81].

5.3 Nedávný vývoj: 12. až 26. listopadu 2026

Tento pododdíl pokrývá výhradně **patnáctidenní okno 12. až 26. listopadu 2026** a nevztahuje jeho počty na delší období [S1][S2]. Během těchto patnácti dnů zaznamenal Brandefense **1 771 příspěvků v podsvětí označených pro Česko** (včetně **53 příspěvků na fórech**, ne všech cílených na Česko) [S1]. Ransompedia ve stejném okně zapsala **tři české záznamy**: opakovanou položku `INC Ransom` pro `Partners Financial Services` z 12. listopadu plus dva neověřené záznamy [S2]. Aktivita na fórech zahrnovala `19. listopadu 1.5K mail access` , `21. listopadu SMS Arena české SIM` a `22. listopadu` recyklované inzeráty `~105K` e-shopu [S1]. Současně se rozvinuly tři velké veřejně potvrzené české incidenty (`Případy P, Q a R`) [S52][S55][S57].

PŘÍPAD P

P

Únik ze Studijního informačního systému Univerzity Karlovy

Vysoké školství

Potvrzený únik

Klíčové ponaučení

Izolujte webové aplikace od centrálních studijních databází, omezte oprávnění databázových účtů a odlišujte kyberútoky od cloudových výpadků.

Dne **13. listopadu 2026** zneužil útočník zranitelnost ve webové aplikaci **Univerzity Karlovy** k přístupu a stažení dat z centrálního **Studijního informačního systému (SIS)** včetně osobních údajů [S52][S53][S54]. Z preventivních důvodů univerzita vyzvala přibližně **55 000 studentů a zaměstnanců** ke změně hesel v Centrální autentizační službě (**CAS**) [S53][S54]. Navazující oficiální prohlášení univerzity upřesnila, že **neexistují důkazy o plošné krádeži hesel CAS**, zatímco Policie ČR a NÚKIB zahájily šetření [S52][S53][S54].

Krizové komunikátory by mělo zaujmout důležité rozlišení ze stejného dne **13. listopadu** [S54]. IT výpadek zasáhl česká ministerstva **financí, dopravy a školství**, avšak **Microsoft Česko potvrdil interní technickou příčinu, nikoli kybernetický útok** [S54]. Oddělení souběžných technických výpadků od potvrzených průniků zabraňuje zmatení veřejnosti a chrání zaměření vyšetřování [S54].

PŘÍPAD Q

Q

Únik starší zálohy e-shopu Dedoles přes slovenského IT dodavatele ui42

Přeshraniční dodavatel e-commerce

Únik u dodavatele

Klíčové ponaučení

Včas mažte zálohy odstavených e-shopů, vyžadujte MFA pro všechny účty externích IT agentur a kontrolujte přeshraniční přístupy.

Mezi **20. a 23. listopadem 2026** oznámil slovenský prodejce oblečení **Dedoles** únik dat přes dodavatele [S55][S56]. Značka výrazně působí i v Česku [S55]. Útočník zneužil ukradené zaměstnanecké přihlašovací údaje u slovenského IT dodavatele `ui42` ke zkopírování zálohy **starší databáze e-shopu** [S55][S56]. Odcizený archiv obsahoval objednávky a fakturační údaje od **září 2021 do června 2026** (jména, kontakty, adresy, zakoupené zboží, čísla faktur a způsob platby) českých a slovenských zákazníků [S55][S56]. Dedoles uvedl, že současný e-shop (provozovaný po červenci 2026), hesla ani platební karty nebyly zasaženy, zrušil přístupy dodavatele a varoval zákazníky před phishingem využívajícím skutečné objednávky [S55][S56].

R

PŘÍPAD R

Ransomwarový útok na stavebniny PRO-DOMA a obnova z páskových záloh

Prodej stavebnin

Útok ransomwaru

Klíčové ponaučení

Udržujte offline páskové či neměnné zálohy pro čistou obnovu sítě, vyžadujte MFA pro VPN a oddělte firemní stanice od domácích zařízení.

V noci z **24. na 25. listopadu 2026** zasáhl ransomware významného českého distributora stavebnin **PRO-DOMA** a přinutil všech **173 českých poboček** přejít na prodej tužkou a papírem [S57]. Podle vyjádření společnosti publikovaného Seznam Zprávami vedení **odmítlo s útočníky vyjednávat**, potvrdilo zachování firemních dat na **magnetických páskách** a zahájilo čistou obnovu infrastruktury na **10 až 14 dní** [S57]. Generální ředitel firmy veřejně připsal útok ruské skupině označované jako **Gold Ogre / Aurora** a zmínil možnou souvislost s pracovní stanicí či domácím zařízením [S57]. Tato vyjádření jsou zde uvedena výhradně jako vlastní sdělení společnosti, nikoli jako nezávislá atribuce státního úřadu [S57].

KLÍČOVÉ ZÁVĚRY

01

Náměšť nad Oslavou a PRO-DOMA se obnovily z offline či páskových záloh, Židlochovice a PRO-DOMA udržely provoz v ručním režimu.

02

Chyby webových aplikací a okrajových systémů (WordPress `wp2shell`, PHP2Shell, SIS Univerzity Karlovy) a platformy třetích stran (BitFaktura, Rohlík.cz, Dedoles/`u142`) určovaly úniky dat v roce 2026.

03

V každém veřejném oznámení jasně oddělujte potvrzené kybernetické průniky od souběžných technických výpadků, jak ukázal 13. listopad u Univerzity Karlovy a tří ministerstev.

KAPITOLA 06

Výpadky, hacktivismus a tvrzení versus realita

06

TATO KAPITOLA ODPOVÍDÁ

Jak by měli čeští obránci odlišovat tvrzení hacktivistů od ověřeného dopadu na služby?

0 a 4

DDoS incidenty zaevidované NÚKIB v září a říjnu navzdory hlasitým vlnám na Telegramu

6.1 Chronologie výpadků a milníků odolnosti v Česku v roce 2026 49

6.2 Tempo hacktivistických DDoS a neověřená tvrzení o průmyslových systémech 50

6.3 Tvrzení versus oficiální záznam 50

KAPITOLA 06

Výpadky, hacktivismus a tvrzení versus realita

VE ZKRATCE

Hacktivistické kanály, které NÚKIB označuje za proruské (`NoName057(16)` , `Server Killers` , `Z-Pentest Alliance`), v roce 2026 opakovaně tvrdily, že vyřadily české vládní weby a ovládly průmyslové systémy kolem politických prohlášení a před říjnovými volbami. NÚKIB však v září zaznamenal nula DDoS incidentů a v říjnu čtyři a nezávislé prověrky nenašly důkazy pro masová tvrzení o kamerách a vytápění. Každé tvrzení ověřte z vlastní telemetrie dostupnosti a publikujte klidné zprávy bez přebírání rétoriky aktérů.

6.1 Chronologie výpadků a milníků odolnosti v Česku v roce 2026

7. 1. 2026	Bezpečnostní rada státu vydává prohlášení k mezinárodní muniční iniciativě [S36]
9. 1. 2026	Dvojjazyčný příspěvek `Server Killers` na Telegramu hrozí české veřejné infrastruktuře; NÚKIB hlásí lednovou vlnu DDoS [S1][S9]
9. 3. 2026	Jarní vlna kyberútoků na obce začíná na Městském úřadě Jemnice (ransomware), následují Židlochovice (15. března, ransomware) a Náměšť nad Oslavou [S37][S38][S40]
7. 4. 2026	FBI IC3 a NÚKIB varují před zneužíváním routerů TP-Link skupinou APT28 (`CVE-2023-50224`); Vojenské zpravodajství aktivně zasahuje [S7][S61]
28. 7. 2026	Koncem července zasahuje kyberútok Městský úřad Šumperk a systémy městské policie [S41]
15. 8. 2026	WordPress `wp2shell` (`CVE-2026-63030` , `CVE-2026-60137`) stojí v srpnu za 8 revidovanými významnými českými incidenty [S8][S15]
23. 8. 2026	Kyberútok zasahuje nebankovní dcery skupiny Partners; Partners Banka potvrzuje nedotčenost bankovních systémů [S42][S43]
28. 9. 2026	`NoName057(16)` vede telegramovou vlnu `#OpCzechRepublic` / `#FuckEastwood` do 4. října před obecními a senátními volbami 9. a 10. října [S1][S67]
21. 10. 2026	PHP2Shell (`CVE-2026-109618` , `CVE-2026-109619`) spouští preventivní odstávku Úřadu vlády ČR, omezení ČHMÚ a zásah na ČVUT [S48][S49][S50]
11. 11. 2026	NÚKIB vydává preventivní OT varování k vystaveným řídicím jednotkám chlazení; v Česku žádná oběť do uzávěrky [S51]
13. 11. 2026	Univerzita Karlova oznamuje únik ze SIS; souběžný výpadek tří ministerstev potvrzen jako nekybernetická technická závada Microsoftu [S52][S54]
24. 11. 2026	CZ.NIC a NÚKIB podepisují veřejnoprávní smlouvu k národnímu CSIRT; přes noc zasahuje ransomware 173 poboček PRO-DOMA [S24][S57]

6.2 Tempo hacktivistických DDoS a neověřená tvrzení o průmyslových systémech

V **červenci 2025** narušila mezinárodní policejní operace (**Operation Eastwood** vedená Europolem a Eurojustem za české účasti) infrastrukturu napojenou na `NoName057(16)` [S5][S85]. Hacktivistická aktivita na Telegramu nicméně v roce 2026 přetrvávala v menších nárazových vlnách [S1][S9][S17].

Dne **9. ledna 2026**, dva dny po prohlášení Bezpečnostní rady státu k muniční iniciativě, pohrozil dvojjazyčný anglicko-český příspěvek `Server Killers` na Telegramu české veřejné infrastruktuře [S1][S36]. To odpovídalo lednovému přehledu NÚKIB jmenujícímu skupiny `NoName057(16)` i `ServerKillers` [S9]. Později mezi **28. zářím a 4. říjnem** zveřejňovaly kanály `NoName057(16)` vícejazyčné seznamy cílů `#OpCzechRepublic` a `#FuckEastwood` před obecními a senátními volbami **9. a 10. října** [S1][S67]. Tyto příspěvky tvrdily výpadky českých úřadů a dopravy [S1]. Mezi incidenty hlášenými NÚKIB bylo v září **0 DDoS** a v říjnu **4**, tedy mnohem méně, než naznačovala telegramová tvrzení [S16][S17].

Samostatně publikovaly telegramové kanály napojené na `Z-Pentest Alliance` a spřízněné skupiny neověřená tvrzení o přístupu k českým bezpečnostním kamerám a topným zařízením [S1][S58]. Jednotlivé neověřené příspěvky zmiňovaly kotel o výkonu 850 kW (17. až 18. ledna), výměníkovou stanici (2. května) a sušárnu dřeva (26. října; názvy neověřených provozů jsou skryty) [S1]. Po říjnové mediální vlně citoval server `Lupa.cz` hodnocení společnosti Check Point, že neexistují důkazy potvrzující ovládnutí tisíců českých kamer ani plošné narušení vytápění [S58]. Tento závěr souzní se společným mezinárodním varováním NÚKIB před nadsazováním OT útoků hacktivisty [S19].

6.3 Tvrzení versus oficiální záznam

Čeští obránci čelí opakovanému tlaku dramatických příspěvků na Telegramu, souběžných výpadků a nadsazených záznamů na únikových webech. Následující tabulka staví výrazná tvrzení roku 2026 vedle ověřených faktů.

Tvrzení nebo veřejný dojem	Ověřený stav	Obranná disciplína
Telegramové příspěvky `NoName057(16)` `#OpCzechRepublic` / `#FuckEastwood` tvrdí plošné vyřazení českých veřejných webů (28. září až 4. října) [S1]	Mezi hlášenými incidenty zaevidoval NÚKIB **0 DDoS v září** a **4 v říjnu**; systémový výpadek hlášen nebyl [S16][S17]	Měřte dostupnost vlastním monitoringem a logy scrubbingové ochrany; zveřejňujte věcný stav bez citování hesel aktérů
`Z-Pentest Alliance` a telegramové kanály tvrdí ovládnutí tisíců českých kamer a regulátorů vytápění [S1][S58]	Neověřená tvrzení; nezávislá technická kontrola nepotvrdila masové převzetí kamer ani topení, vystavené OT řídicí jednotky však přesto vyžadují izolaci [S19][S51][S58]	Zmapujte a odpojte vystavená rozhraní HMI, PLC a chlazení z veřejného internetu místo reakcí na snímky z Telegramu
Souběžné výpadky tří ministerstev a Univerzity Karlovy 13. listopadu vnímané jako jeden koordinovaný kyberútok [S54]	Univerzita Karlova potvrdila únik z webové aplikace SIS, zatímco Microsoft Česko potvrdil interní nekybernetickou technickou závadu u ministerstev [S52] [S54]	Ověřte kořenovou příčinu dříve, než spojíte paralelní výpadky v krizových brífincích či hlášeních

Tvrzení nebo veřejný dojem	Ověřený stav	Obranná disciplína
Říjnová nedostupnost webu Úřadu vlády ČR vnímaná jako průnik [S48]	Potvrzeno jako zhruba dvouhodinová preventivní odstávka kvůli PHP2Shell (`CVE-2026-109618` , `CVE-2026-109619`) před záplatováním bez potvrzeného průniku [S48] [S50]	Předem schvalte preventivní odstávky DMZ a veřejně jasně sdělte, kdy jde o preventivní opatření
Příspěvek na fóru z 22. listopadu nabízí databázi českého e-shopu o ~105K řádcích jako „Year: 2026 Fresh" [S1]	Porovnání schématu a časových značek odpovídá inzerátu z 24. února se záznamy končícími 25. listopadu 2025; cíl nepotvrzen [S1]	Před vyhlášením nového úniku porovnejte názvy sloupců a nejnovější časové značky se starším archivem

KLÍČOVÉ ZÁVĚRY

01

NÚKIB zaevidoval 0 DDoS incidentů v září a 4 v říjnu navzdory intenzivní komunikaci `#OpCzechRepublic` na Telegramu.

02

Neověřená tvrzení o kamerách a vytápění postrádala nezávislé důkazy, avšak listopadové varování NÚKIB ke chlazení připomíná nutnost odpojit vystavené OT od internetu.

03

V každém veřejném oznámení oddělujte potvrzené průniky od preventivních odstávek a nekybernetických technických poruch.

KAPITOLA 07

Ransomware, varování před špionáží a profily hrozeb

TATO KAPITOLA ODPOVÍDÁ

Kdo si nárokuje české cíle a co odlišuje vyděračské označení od státního varování?

50

záznamů o ransomwaru označených pro Česko u 20 vyděračských označení

7.1 Regionální záznamy ransomwaru a měsíční koncentrace 53

7.2 Síť hrozeb a profilovaní vyděračští a hacktivističtí aktéři 55

7.3 Varování před státem podporovanou špionáží cílící na Česko 60

KAPITOLA 07

Ransomware, varování před špionáží a profily hrozeb

VE ZKRATCE

Ransompedia zaznamenala mezi 1. lednem a 26. listopadem 2026 celkem 50 vyděračských záznamů označených pro Česko, téměř dvojnásobek oproti 27 za celý rok 2025, s maximem 13 v červenci. Pět záznamů, odpovídajících čtyřem potvrzeným veřejným českým případům (Jemnice, Židlochovice, dvakrát Partners Financial Services a Šumperk), se shoduje s veřejnými zprávami, zatímco 45 tvrzení zůstává neověřených. Varování NÚKIB a spojenců dokumentují špionážní kampaně využívající známé chyby a slabou autentizaci. Posilte zálohy, záplatujte §12.2 a ověřujte každé vyděračské tvrzení interně.

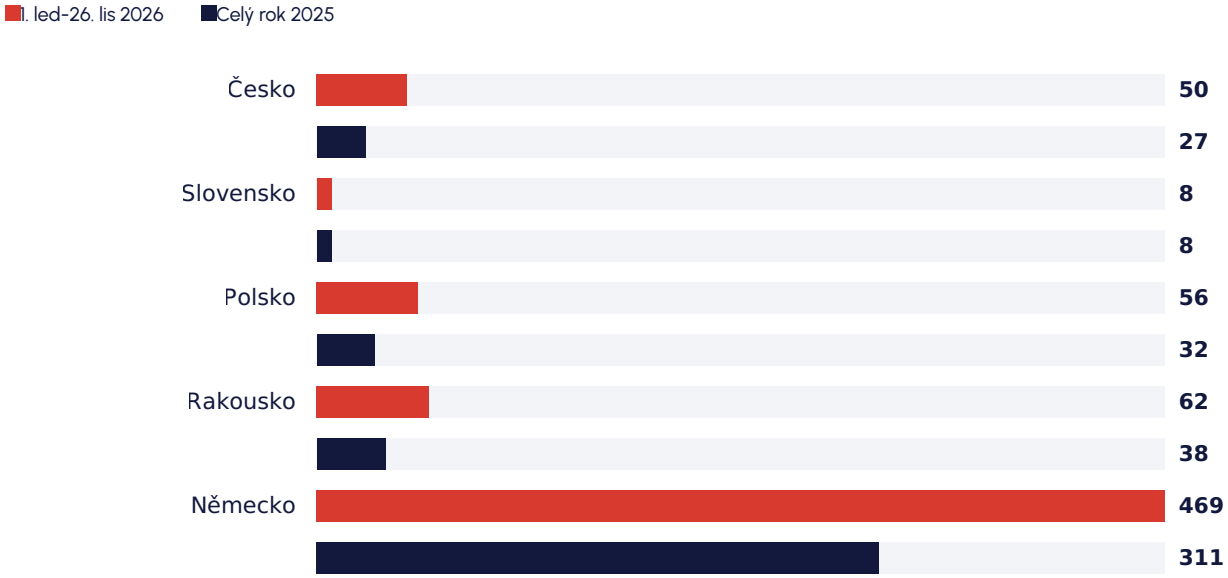
7.1 Regionální záznamy ransomwaru a měsíční koncentrace

Mezi **1. lednem a 26. listopadem 2026** zaevidovala Ransompedia **50 vyděračských záznamů označených pro Česko** napříč **20 označeními skupin**, oproti **27 záznamům** za celý rok 2025 (**119** od počátku sledování) [S2]. Tento vzestup souzní s přehledem ESET Česko za Q1 2026, který zaznamenal stoprocentní meziroční nárůst na 12 evidovaných českých obětí ransomwaru za první čtvrtletí [S59]. Měsíční počty Ransompedia činily: leden **3**, únor **3**, březen **5**, duben **5**, květen **1**, červen **2**, **červenec 13**, srpen **6**, září **5**, říjen **4** a částečný listopad **3** [S2]. Tři listopadové záznamy zahrnují jeden opakovaný potvrzený záznam a dva neověřené záznamy [S2].

Dva opakované záznamy snižují celkových 50 položek na **nejvýše 48 různých nárokovaných subjektů** [S2]. Konkrétně `Partners Financial Services, a.s.` se objevila dvakrát pod **INC Ransom** (`16. září` a `12. listopadu`) a jeden neověřený subjekt (skrytý) se objevil dvakrát pod dvěma různými označeními [S2][S42]. Ze všech 50 záznamů odpovídá veřejným zprávám pouze **pět položek** (čtyři potvrzené veřejné české případy v kapitole 5) [S2].

Těchto pět položek pokrývá **Městský úřad Jemnice** (`Lockbit5`, 6. dubna), **Městský úřad Židlochovice** (`Deadlock`, 10. července), **Partners Financial Services** (`INC Ransom`, 16. září a 12. listopadu) a **Městský úřad Šumperk** (`Safepay`, 28. září) [S2][S37][S38][S41][S42]. Zbývajících **45 položek** (nejvýše **44 různých subjektů**) nemá veřejné české potvrzení a zůstává přísně neověřených a skrytých [S2]. Také sektorové značení únikových webů bývá chybné: Židlochovice (`medias-and-audiovisual`) i Šumperk (`retail-and-commerce`) byly portály zařazeny chybně [S2].

50 českých záznamů o ransomwaru téměř zdvojnásobuje rok 2025 a zaostává za Polskem, Rakouskem a Německem



Zdroj: Brandefense Ransompedia, 1. ledna–26. listopadu 2026 oproti celému roku 2025 [S2]. Nestejně dlouhá období; tvrzení označená podle zemí, nikoli unikátní oběti, potvrzené průniky ani národní bezpečnostní žebříček.

Srovnávací země byly vybrány jako příklady výhradně pro poskytnutí kontextu; jejich výběr neznamená žebříček ani politické hodnocení.

Ve srovnání se čtyřmi sousedními zeměmi za stejné období roku 2026 (oproti celému roku 2025) stojí Česko mezi Slovenskem a většími či bohatšími sousedy [S2]:

Země	Záznamy v okně 2026 (1. led–26. lis)	Záznamy za celý rok 2025	Nejčastější označení v roce 2026	Zdroje
Česko (CZ)	**50**	**27**	The Gentlemen (16), Titan (4), Krybit (3), Lockbit5 (3), AKIRA (3), Qilin (3), Deadlock (3), INC Ransom (2), Safepay (2)	[S2]
Slovensko (SK)	8	8	Qilin (2), APT73 (2), The Gentlemen (1), Safepay (1), Clop (1), INC Ransom (1)	[S2]
Polsko (PL)	56	32	The Gentlemen (19), Deadlock (5), Coinbasecartel (4), Nova (4), Qilin (3)	[S2]
Rakousko (AT)	62	38	The Gentlemen (11), Qilin (9), Lockbit5 (8), Krybit (4), Payload (4)	[S2]
Německo (DE)	469	311	Qilin (63), Safepay (58), The Gentlemen (48), AKIRA (29), Payload (20)	[S2]

Skupina **The Gentlemen** vedla v Česku (**16 záznamů**, 32 %), Polsku (**19**) i Rakousku (**11**) a byla třetí v Německu (**48**), což odráží regionální středoevropskou vlnu vydírání spíše než izolovaný domácí výkyv [S2]. Jedenáct dalších označení se v Česku v roce 2026 objevilo po jednom záznamu (úplné počty uvádějí data grafu c08) [S2]. Noční ransomwarový útok na PRO-DOMA z 24. na 25. listopadu (`Případ R`) se do uzávěrky 26. listopadu v Ransompedia neobjevil, ačkoli společnost útok veřejně připsala jmenované ruské skupině (§5.3) [S2][S57].

7.2 Síť hrozeb a profilovaní vyděračští a hacktivističtí aktéři

Síťový diagram a karty skupin níže rozlišují finančně motivovaná vyděračská označení, hacktivistické kanály a státem připisované špionážní shluky aktivní kolem Česka v roce 2026.

Vlastní příspěvek Přeposlání Oficiální varování Veřejné zdroje Vlastní pozorování

The Gentlemen

Vlastní data
16 záznamů, S2 ↓

Záznamy pro Česko (50)

Vlastní data
2 opakované záznamy, S2 ↑

INC Ransom

Deadlock

Vlastní data
3 záznamy (včetně potvrzeného případu obce), S2, S38 ↓

Záznamy pro Česko (50)

Vlastní data
3 záznamy (včetně potvrzeného případu obce), S2, S37 ↑

Lockbit5

NoName057(16) a ServerKillers

Oficiální
Lednová vlna DDoS a 42 incidentů od roku 2023, S9, S19 ↑

Oficiální česká a spojenecká varování

Oficiální
Varování k VNC/OT z prosince 2025 a Q1 2026, S6, S19 ↓

Z-Pentest Alliance

Varování GRU / APT28

Oficiální
Dubnový zásah u routerů TP-Link, S7, S61 ↑

Oficiální česká a spojenecká varování

Oficiální
Varování Q3 2026 k Zimbra a Signal / Device Code, S8, S18 ↓

LAUNDRY BEAR a STORM-2372

SparkyCarp a varování k ČLR

Oficiální
Přehledy Q2–Q3 2026 k Evropským hodnotám a BlueMoon, S7, S8 ↑

Oficiální česká a spojenecká varování

The Gentlemen

Thegentlemen (označení v pozorovaných záznamech)

Označení ransomwarového a vyděračského portálu | Státní atribuce není prokázána

V ČESKU, 2026

Období 2026

16 záznamů označených pro Česko (32,0 % z 50), leden–listopad 2026, S2

1. 4. 2026

ESET Česko zařadil skupinu mezi tři nejaktivnější RaaS gangy cílící na ČR, S59

UVÁDĚNÉ CÍLE

Záznamy pro Česko napříč několika sektory (všech 16 nepotvrzených; totožnost, sektor i datum skryty)

VE VEŘEJNÝCH ZDROJÍCH

[S2] 16 českých záznamů v Ransompedii v roce 2026

[S59] Tisková zpráva ESET Česko k 1. čtvrtletí 2026 jmenující Gentlemen, Akira a Qilin

NAŠE HODNOCENÍ

The Gentlemen představuje v roce 2026 nejčetnější označení mezi 50 českými záznamy v Ransompedii (16 z 50). Zápis na vyděračském portálu dokládá pouze tvrzení útočníka, nikoli potvrzené zašifrování, únik dat nebo přesné zařazení sektoru.

SPOLEHLIVOST

Vysoká pro zaznamenaný počet a zprávu ESET; jednotlivá nepotvrzená tvrzení zůstávají neověřená

INC Ransom

Označení v pozorovaných záznamech

Označení ransomwarového a vyděračského portálu | Státní atribuce není prokázána

V ČESKU, 2026

Září a listopad 2026

2 opakované záznamy pro Česko (16. září a 12. listopadu) odpovídající potvrzenému incidentu nebankovní dceřiné společnosti Partners Financial Services, S2, S42, S43

UVÁDĚNÉ CÍLE

Nebankovní finančněporadenská společnost (Partners Financial Services potvrdila srpnový kyberútok; Partners Banka nebyla zasažena)

VE VEŘEJNÝCH ZDROJÍCH

[S2] 2 opakované záznamy v Ransompedii (16. září a 12. listopadu)

[S42] Oficiální sdělení Partners Banky potvrzující zásah nebankovních dceřiných firem

[S43] Zpravodajství Novinky.cz o incidentu skupiny Partners

NAŠE HODNOCENÍ

Zářijový a listopadový zápis INC Ransom dokládá, jak opakované zveřejnění nadhodnocuje hrubé počty obětí a zároveň navazuje na potvrzený srpnový incident. Skupina Partners potvrdila přístup k osobním údajům v nebankovních firmách a vyloučila zásah Partners Banky.

SPOLEHLIVOST
Vysoká pro zaznamenané opakování a oficiální sdělení firmy; rozsah souborů u útočníků zůstává neověřen

Deadlock

Označení v pozorovaných záznamech

Označení ransomwarového a vyděračského portálu | Státní atribuce není prokázána

V ČESKU, 2026

15. 3. 2026
Potvrzený útok ransomwaru Deadlock narušil provoz Městského úřadu Židlochovice, S38, S39

Období 2026
3 záznamy označené pro Česko v Ransompedii včetně potvrzeného záznamu Židlochovic, S2

UVÁDĚNÉ CÍLE

Potvrzený městský úřad (Židlochovice) a dva nepotvrzené záznamy (totožnost, sektor i datum skryty)

VE VEŘEJNÝCH ZDROJÍCH

[S2] 3 záznamy pro Česko v Ransompedii v roce 2026

[S38] Zpráva Novinky.cz potvrzující ransomware Deadlock na radnici v Židlochovicích

[S39] Navazující reportáž Seznam Zpráv o měsíční obnově a hotovostním provozu

NAŠE HODNOCENÍ

Březnové potvrzení v Židlochovicích a červencový zápis na vyděračském webu ukazují několikaměsíční odstup mezi zašifrováním a zveřejněním i nepřesnost sektorových štítků (radnice byla zařazena mezi média).

SPOLEHLIVOST
Vysoká pro potvrzený případ Židlochovic a zaznamenaný počet; ostatní záznamy zůstávají neověřené

Lockbit5

Označení v pozorovaných záznamech

Označení ransomwarového a vyděračského portálu | Státní atribuce není prokázána

V ČESKU, 2026

9. 3. 2026
Potvrzený ransomwarový útok na Městský úřad Jemnice; zapsán 6. dubna pod Lockbit5, S2, S37

Období 2026
3 záznamy pro Česko v Ransompedii včetně potvrzeného záznamu Jemnice, S2

UVÁDĚNÉ CÍLE

Potvrzený městský úřad (Jemnice) a dva nepotvrzené záznamy (totožnost, sektor i datum skryty)

VE VEŘEJNÝCH ZDROJÍCH

[S2] 3 záznamy pro Česko v Ransompedii

[S37] Zpráva Novinky.cz potvrzující ransomwarový útok na Městský úřad Jemnice

NAŠE HODNOCENÍ

Spolu se skupinami Deadlock a Safepay (která zapsala Šumperk po potvrzeném červencovém průniku) dokládá Lockbit5 trvalý ransomwarový tlak na české obce v režimu nižších povinností.

SPOLEHLIVOST
Vysoká pro potvrzený případ Jemnice a zaznamenaný počet; ostatní záznamy zůstávají neověřené

NoName057(16) a ServerKillers

DDoSia Project (označení telegramového kanálu)

Haktivistické DDoS skupiny | NÚKIB a Europol je označují za proruské haktivistické skupiny

V ČESKU, 2026

Leden 2026
NÚKIB je jmenoval jako hlavní původce lednového maxima 32 incidentů (téměř polovina DDoS), S6, S9

UVÁDĚNÉ CÍLE

České vládní portály, systémy veřejných zakázek, regionální dopravní podniky, energetické a logistické weby

9. 1. 2026
Server Killers zveřejnili anglicko-českou výhrůžku českým vládním webům s odkazem na dodávky munice, S1

Září–říjen 2026
Vícejazyčná vlna DDoS tvrzení (#OpCzechRepublic, #FuckEastwood), zatímco NÚKIB v září evidoval 0 DDoS a v říjnu 4, S1, S16, S17

VE VEŘEJNÝCH ZDROJÍCH

[S1] Pozorované telegramové výhrůžky a odkazy check-host (leden, březen, září–říjen)

[S9] Lednový přehled incidentů NÚKIB jmenující NoName057(16) a ServerKillers

[S19] Varování NÚKIB z prosince 2025 uvádějící 42 incidentů NoName057(16) v ČR od roku 2023

[S85] Zpráva ČT24 o mezinárodní operaci Eastwood (červenec 2025)

NAŠE HODNOCENÍ

Navzdory červencovému mezinárodnímu zásahu v rámci operace Eastwood (s českou účastí) vyvolaly skupiny NoName057(16) a ServerKillers lednový vrchol DDoS útoků, načež v evidenci NÚKIB výrazně oslabily. Zářijová tvrzení na Telegramu dalece převyšovala DDoS incidenty hlášené NÚKIB.

SPOLEHLIVOST
Vysoká pro statistiky NÚKIB a pozorované příspěvky; jednotlivá nepotvrzená tvrzení zůstávají neověřená

Z-Pentest Alliance

Z-Alliance (označení telegramového kanálu)

Haktivistická skupina nárokující průniky do OT | NÚKIB a FBI ji označují za proruskou haktivistickou skupinu cílící na vystavené OT systémy

V ČESKU, 2026

Leden, květen a říjen 2026
Neověřená telegramová tvrzení o přístupu k řídicím systémům české teplárny, kotle, výměníkové stanice a sušárny dřeva, S1

Q1 2026
NÚKIB varoval před zneužíváním slabě zabezpečených rozhraní VNC na PLC zařízeních s minimálním dopadem u neregulovaných subjektů, S6

UVÁDĚNÉ CÍLE

Nedostatečně zabezpečená rozhraní VNC a HMI vystavená do internetu v menších teplárenských, vodohospodářských a průmyslových provozech

VE VEŘEJNÝCH ZDROJÍCH

[S1] Pozorované telegramové příspěvky s OT tvrzeními (leden, květen, říjen 2026)

[S6] Čtvrtletní přehled NÚKIB Q1 2026 k vystaveným rozhraním VNC/PLC

[S19] Společné varování NÚKIB a FBI jmenující Z-Pentest, CARR a NoName057(16)

NAŠE HODNOCENÍ

Pozorovaná tvrzení z ledna, května a října zapadají do varování NÚKIB před vystavenými službami VNC, nikoli do velkých výpadků infrastruktury. Odpojení VNC od veřejného internetu odstraňuje hlavní vstupní cestu.

SPOLEHLIVOST
Vysoká pro oficiální varování a pozorovaná tvrzení; jednotlivá tvrzení o konkrétních provozech zůstávají neověřená

7.3 Varování před státem podporovanou špionáží cílící na Česko

Každá státní atribuce v této kapitole je uváděna výhradně jako atribuce citovaného oficiálního úřadu. Ve svých čtvrtletních přehledech roku 2026 a v **Analýze hrozeb z 20. října 2026** zdůraznil NÚKIB stálý provozní vzorec [S6] [S7][S8][S18]. Státem podporovaní aktéři cílící na česká ministerstva, nevládní organizace a soukromé firmy kombinují výběrové špionážní nástroje s rutinním zneužíváním známých chyb, slabých hesel a phishingu [S18]. Mnohým průnikům lze zabránit základní hygienou [S18].

Ruskem podporovaná aktivita (podle NÚKIB a FBI IC3). V Q1 2026 sledoval NÚKIB skupinu **APT28** (`Operation Neusploit`) zneužívající obcházení bezpečnostní funkce v Microsoft Office `CVE-2026-21509` (CVSS 7,8, CISA KEV) [S6][S18][S82]. V dubnu popsaly FBI IC3 (`PSA260407`) a přehled NÚKIB za Q2 zneužívání starších **SOHO routerů TP-Link** (`CVE-2023-50224`) skupinou GRU / **APT28**, proti kterému aktivně zasáhlo Vojenské zpravodajství [S7] [S61][S62][S84]. V Q3 a analýze z 20. října dále NÚKIB upozornil na **APT28** (`HOOKEDGE`) a **STORM-2372** (cílený na účty Signal a Microsoft 365 Device Code Flow) [S8][S18]. Stejná varování zachytila **LAUNDRY BEAR** zneužívající uložené XSS v Zimbra Collaboration Classic UI `CVE-2025-66376` (CVSS 6,1/7,2, CISA KEV) [S8][S18][S83].

Aktivita napojená na ČLR a zadní vrátka v routerech (podle NÚKIB). Atribuce průniku do neutajované sítě MZV (2022–2024) skupině **APT31** z května 2025 slouží výhradně jako kontext před rokem 2026 [S5]. V rámci roku 2026 zdokumentoval přehled NÚKIB za Q2 phishing **SparkyCarp** proti českému think-tanku **Evropské hodnoty**, spojený se sběrem zaměřeným na **Tchaj-wan** (bez jmenování jednotlivců) [S7]. V Q3 2026 NÚKIB dále popsal exploit kit **BlueMoon** pro prohlížeče a Windows spojovaný s **APT31** a třemi dalšími aktéry napojenými na ČLR [S8]. Zpráva zároveň popsala zadní vrátka ve firmwaru routerů **Tenda** (oznámená CERT/CC) a zařízeních **Zbtlink** (`ENDLESSDOORS`) [S8].

GRU / APT28 (oficiální varování)

Fancy Bear, Forest Blizzard, Sofacy (označení úřadů)

Státem sponzorovaný špionážní aktér (oficiální varování) | FBI, NÚKIB a Vojenské zpravodajství jej připisují ruské vojenské rozvědce (GRU)

V ČESKU, 2026

Q1 2026

Přehled NÚKIB Q1 popsal kampaň Operation Neusploit (CVE-2026-21509) proti evropským cílům včetně Slovenska a Polska, S6

Duben 2026

Vojenské zpravodajství provedlo aktivní zásah k zabezpečení zneužitých routerů TP-Link (CVE-2023-50224), S7, S61

Q3 2026

Přehled NÚKIB Q3 popsal backdoor HOOKEDGE proti evropským diplomatickým cílům (střední jistota Recorded Future), S8

UVÁDĚNÉ CÍLE

SOHO routery (CVE-2023-50224), uživatelé Microsoft Office (CVE-2026-21509), vládní, vojenské a kritické instituce

VE VEŘEJNÝCH ZDROJÍCH

[S6] Čtvrtletní přehled NÚKIB Q1 2026 (Operation Neusploit)

[S7] Čtvrtletní přehled NÚKIB Q2 2026 (aktivní zásah Vojenského zpravodajství)

[S8] Čtvrtletní přehled NÚKIB Q3 2026 (backdoor HOOKEDGE)

[S61] Varování FBI IC3 PSA260407 k routerům

[S84] Záznam NVD pro CVE-2023-50224

NAŠE HODNOCENÍ

Aktivní zásah českého Vojenského zpravodajství na zneužitých routerech TP-Link v Česku činí dubnové varování k GRU/APT28 přímo provozně relevantním. Veškeré státní atribuce zůstávají výhradně hodnocením citovaných úřadů.

SPOLEHLIVOST

Vysoká pro oficiální varování úřadů; bez nezávislé atribuce či celkového počtu českých obětí

LAUNDRY BEAR a STORM-2372 (přehled NÚKIB Q3)

Špionážní skupiny napojené na Rusko (označení úřadů)

Státem přisuzované špionážní skupiny (oficiální varování) | NÚKIB a zahraniční partneři je spojují s aktéry napojenými na Ruskou federaci

V ČESKU, 2026

Q3 2026

NÚKIB se připojil ke společnému varování před skupinou LAUNDRY BEAR zneužívající Zimbra Collaboration Suite (CVE-2025-66376) nejméně od července 2025, S8, S18

Q3 2026

NÚKIB varoval před phishingem skupiny STORM-2372 přes Signal a zneužíváním Microsoft Entra ID Device Code Flow proti činitelům a bezpečnostním složkám, S8

UVÁDĚNÉ CÍLE

Vládní instituce, obranný průmysl, energetika, média, školství, nevládní organizace a úředníci používající Signal, Microsoft 365 či Zimbra

VE VEŘEJNÝCH ZDROJÍCH

[S8] Čtvrtletní přehled NÚKIB Q3 2026 (Signal, Device Code Flow, Zimbra)

[S18] Analýza hrozeb NÚKIB z října 2026 k ruským státním aktérům

[S83] Záznam NVD pro CVE-2025-66376

NAŠE HODNOCENÍ

Přehled Q3 i říjnová analýza NÚKIB zdůrazňují, že státem přisuzovaná kyberšpionáž proti českým a aliančním cílům silně spoléhá na neaktualizovaný webmail, sociální inženýrství v aplikaci Signal a zneužití OAuth Device Code Flow.

SPOLEHLIVOST

Vysoká pro zveřejněná varování NÚKIB; celkový počet českých obětí nebyl zveřejněn

SparkyCarp a varování k ČLR (včetně historického APT31)

UNK_SparkyCarp, APT31 (označení úřadů)

Státem přisuzovaná špionážní varování | NÚKIB a české orgány je připisují aktérům napojeným na Čínskou lidovou republiku

UVÁDĚNÉ CÍLE

České think-tanky, nevládní organizace, zahraničněpolitické instituce a webové prohlížeče či síťové prvky

V ČESKU, 2026

Q2 2026

NÚKIB popsal pokus skupiny SparkyCarp o phishing přihlašovacích údajů u českého think-tanku Evropské hodnoty (NÚKIB jej spojil s širší kampaní zaměřenou na Tchaj-wan), S7

Q3 2026

NÚKIB upozornil na exploit kit BlueMoon pro Chrome a Windows sdílený nejméně čtyřmi aktéry spojovanými s ČLR včetně APT31, S8

Kontext květen 2025

Historická česká státní atribuce skupiny APT31 za průnik do neutajované sítě MZV v letech 2022–2024 (před rokem 2026), S5

VE VEŘEJNÝCH ZDROJÍCH

[S5] Zpráva NÚKIB za rok 2025 (historická atribuce APT31 z května 2025)

[S7] Čtvrtletní přehled NÚKIB Q2 2026 (SparkyCarp a Evropské hodnoty)

[S8] Čtvrtletní přehled NÚKIB Q3 2026 (exploit kit BlueMoon a zadní vrátka v routerech Tenda a Zbtlink)

NAŠE HODNOCENÍ

Přehledy NÚKIB za Q2 a Q3 2026 uvádějí phishing napojený na ČLR proti české politické organizaci i zneužívání časové mezery v záplatování prohlížečů a zadních vrátek v routerech. Průnik na MZV z let 2022–2024 patří do kontextu před rokem 2026.

SPOLEHLIVOST

Vysoká pro oficiální zprávy NÚKIB; státní atribuce zůstávají výhradně hodnocením citovaných úřadů

KLÍČOVÉ ZÁVĚRY

01

50 českých záznamů Ransompedia téměř zdvojnásobilo počet 27 za rok 2025 v čele s The Gentlemen (16), avšak 45 z 50 tvrzení zůstává neověřených.

02

Pět záznamů pokrývajících čtyři potvrzené české incidenty odpovídalo položkám Ransompedia, dva z nich s chybně přiřazeným sektorem.

03

Varování NÚKIB a FBI IC3 uvádějí, že mnoho státem připisovaných průniků využívá známé chyby Office, Zimbry a routerů a zneužití Device Code Flow; jejich záplatování a blokování uzavírá běžné vstupní cesty.

KAPITOLA 08

Podvody, zneužití identity a druhotné škody

TATO KAPITOLA ODPOVÍDÁ

Jak uniklé osobní údaje a služby z podsvětí pohánějí českou podvodnou ekonomiku?

11,8 mld. Kč

pokusů o české bankovní podvody v 75 637 útocích v Q1 až Q3 2026

8.1 Národní rozsah digitálních podvodů a posun taktik útočníků 65

8.2 Padělané české doklady, sady KYC a nastrčené společnosti 65

8.3 Platební karty: úzké pozorování 68

8.4 Druhotné škody po potvrzených českých únicích dat 68

KAPITOLA 08

Podvody, zneužití identity a druhotné škody

VE ZKRATCE

Kyberpodvody jsou v roce 2026 nejobjemnější finanční hrozbou v Česku. Policie ČR v roce 2025 zaevidovala 21 137 případů (+14,3 %) a v březnu 2026 rekordních 2 533 případů. Banky v Česku zastavily 81 % z 11,8 miliardy Kč v pokusech za Q1 až Q3, ale klienti ztratili 2,2 miliardy Kč. Podsvětí dodává padělané výplatní pásky, KYC selfie, nastrčené firmy a SIM, zatímco reálné úniky živí podvody. Zpřísněte ověřování účtů.

8.1 Národní rozsah digitálních podvodů a posun taktik útočníků

Oficiální české policejní, bankovní a telekomunikační statistiky kreslí jednotný obraz rostoucího sociálního inženýrství spojeného s rychlou změnou kanálů. V roce 2025 zaevidovalo Ministerstvo vnitra **21 137 kybernetických trestných činů** (+2 642 čili **+14,3 %** meziročně), což představovalo **12,4 %** veškeré kriminality při poklesu celkové kriminality o 1,9 % [S25]. Objasněnost činila jen **15,1 %**, což odráží přeshraniční infrastrukturu a rychlý výběr přes bílé koně [S25]. V **březnu 2026** zaznamenala policie historické měsíční maximum **2 533 kybernetických případů** (+37 % meziročně), přičemž hlasové podvody falešných bankéřů a policistů stály oběti v první části roku 2026 celkem **322 milionů Kč** [S26].

Bankovní statistiky potvrzují vysokou míru zachycení i citelné zbytkové škody. Za **Q1 až Q3 2026** nahlásila Česká bankovní asociace (ČBA) **75 637 útoků** (+7 611 meziročně) s cílem odcizit **11,8 miliardy Kč** [S29][S30]. Banky ochránily **9,6 miliardy Kč (81 %)**, ale klienti přesto přišli o **2,2 miliardy Kč** [S29][S30]. Průměrná škoda dosáhla **29 266 Kč** na jeden úspěšný podvod [S30]. Testování ČBA a Ipsos určilo český Index kyberbezpečnosti na **62** celkově a **59** u dospělých ve věku 18 až 34 let [S30]. Samotná digitální zběhlost mladší uživatele před naléhavým sociálním inženýrstvím nechrání [S30].

Regulační zásahy v telekomunikacích proměnily v letech 2025 a 2026 doručovací kanály útočníků. Regulátor ČTÚ (Český telekomunikační úřad) zavedl protispoofingová pravidla pro pevné linky [S34]. Novela zákona o elektronických komunikacích z července 2025 pak umožnila blokovat podvržená zahraniční volání s českou předvolbou [S35]. Operátoři tak nyní filtrují **miliony pokusů o podvodná volání měsíčně** [S34][S35].

V reakci na to varovaly ČTÚ, NÚKIB, Bank iD i Portál veřejné správy před prudkým posunem ke **smishingu**, phishingovým e-mailům a falešným přihlášením na Portál občana [S7][S31][S32][S34]. Kampaně často napodobují Policii ČR (s využitím domén `.cfd`, `.bond` a `.xyz`), vrácení daní, poštovní zásilky a bankovní výstrahy [S7][S32]. Samostatně zaznamenal ÚOOÚ v roce 2025 celkem **1 430 stížností na spam** a uložil pokuty za přímý marketing ve výši **12,1 milionu Kč** [S33].

8.2 Padělané české doklady, sady KYC a nastrčené společnosti

Inzeráty zachycené v roce 2026 dodávají přesné doklady a firemní schránky potřebné k obcházení vzdáleného ověřování totožnosti a praní peněz v Česku [S1].

Karta důkazu B10 — 21. 8. 2026

Autor na fóru (přezdívka skryta) | Fórum | Fórum | Angličtina

ORIGINÁL

Update - new for Czech Republic: - proof of address - utility bill - proof of income - payslip

PŘEKLAD

Aktualizace – nově pro Českou republiku: potvrzení adresy, vyúčtování energií, potvrzení příjmu, výplatní páska

Poznámka. Odkazy na vlákno jsou odstraněny; dokládá, proč statické PDF doklady vyžadují nezávislé ověření.

Doloženo
Srpnová aktualizace na fóru rozšiřuje komerční službu padělání dokumentů o české potvrzení adresy, faktury za energie, potvrzení příjmu a výplatní pásky na zakázku.

Neprokázáno
Úspěšné obejití kontrol konkrétní české banky, úvěrové společnosti nebo poskytovatele ověření identity.

Karta důkazu B11 — 19. 8. 2026

Autor na fóru (přezdívka skryta) | Fórum | Fórum | Angličtina

ORIGINÁL

DIGITAL KYC Documents for your VERIFICATION NEEDS ID Front + Back Selfie Pictures $15 per US -- $20 with SSN $25 per EU [...] Countries Listed Down Below: Austria Belgium Brazil Czech Repub [...] Polish [...] Romanian Spain

PŘEKLAD

Digitální KYC doklady pro ověření – přední a zadní strana průkazu se selfie: 15 USD USA, 20 USD s SSN, 25 USD EU [...] Seznam zemí: Rakousko, Belgie, Brazílie, Česká republika [...] Polsko [...] Rumunsko, Španělsko

Poznámka. Identifikátory komunikátorů jsou odstraněny; samostatná lednová a únorová vlákna šířila také balíčky českých průkazů se selfie a 33 sad pasů.

Doloženo
Srpnový prodejce na fóru nabízí evropské balíčky přední a zadní strany průkazu totožnosti se selfie včetně Česka za 25 USD, vedle dubnového náboru platícího 30 USD za živé KYC skeny přes odkaz.

Neprokázáno
Pravost dokladů totožnosti, původ fotografií ani úspěšné založení finančního účtu.

Karta důkazu B12 — 12. 1. 2026

Autor na fóru (přezdívka skryta) | Fórum | Fórum | Ruština

ORIGINÁL

Оформление ИП и компаний на заказ в СНГ и Европе [...] Польша. ИП 3500$, ООО 4900$. Чехия. ИП 3500$, ООО 4900$. Стандартная комплектация материала: Банковский счёт. ЭЦП на токене. Паспорт...

PŘEKLAD

Zakládání živností a společností na zakázku v SNS a Evropě [...] Polsko: živnost 3 500 USD, s.r.o. 4 900 USD. Česko: živnost 3 500 USD, s.r.o. 4 900 USD. Standardní sada: bankovní účet, elektronický podpis na tokenu, pas...

Poznámka. Samostatný zářijový příspěvek na fóru nabízel také síť bílých koní a pracovníků pro KYC uvádějící Česko a Slovensko.

Doloženo
Ruskojazyčný prodejce na fóru inzeruje zakládání nastrčených českých živností (3 500 USD) a společností s ručením omezeným (4 900 USD) v balíčku s bankovním účtem a hardwarovým tokenem elektronického podpisu.

Neprokázáno
Skutečné zápisy v českém živnostenském či obchodním rejstříku, aktivní schránkové firmy ani úspěšné založení firemních účtů.

V zaznamenaných příspěvcích se opakují tři komerční vrstvy podvodných vstupů (`Případ F`) [S1]:

- **Zakázkové padělky domácích dokladů (`B10`).** Dne **21. srpna 2026** nabízel prodejce české doklady o adrese, vyúčtování energií, bankovní výpisy a výplatní pásky připravené pro kontroly úvěrů a zakládání účtů [S1].
- **Levné ověřovací sady EU KYC (`B11`).** Dne **19. srpna** nabízeli prodejci **sady EU KYC dokladů a selfie za 25 USD** pokrývající Česko [S1]. To doplňovalo dubnový nábor (`19. dubna`) platící **30 USD** za živé ověřovací odkazy pro platební a krypto účty [S1].
- **Hotové české nastrčené firmy (`B12`).** Dne **12. ledna** nabízel prodejce nastrčené **české OSVČ za 3 500 USD** a **české s.r.o. za 4 900 USD** [S1]. Inzerát uváděl dodání s firemními účty a tokeny elektronického podpisu [S1]. V kombinaci s českými eSIM (`11. února`) a pronájmem fyzických SIM `SMS Arena` (`21. listopadu` , `Případ E`) sestavují sítě syntetické identity bez návštěvy pobočky [S1].

8.3 Platební karty: úzké pozorování

ROZSAH ÚDAJŮ O KARTÁCH

Tyto údaje popisují omezenou pozorovanou publikační populaci. Neodhadují krádeže českých karet, celostátní ztráty z podvodů ani živou platnost karet.

Mezi **1. lednem a 26. listopadem 2026** zachytil Brandefense **42 různých záznamů platebních karet označených pro Česko** [S1]. Objevily se v **60 výskytech napříč 55 příspěvky** a pokrývaly **21 různých šestimístných BIN kódů** [S1]. Podle karetní sítě a uvedeného typu se těchto 42 záznamů dělí na **33 Mastercard** a **9 Visa**, a dále na **25 debetních**, **4 kreditní**, **1 předplacenou** a **12 neoznačených** karet [S1].

Podle publikačního kanálu (jedna karta se může objevit na více místech) se **29** různých karet objevilo ve výstupech automatických kontrolních botů, **14** v chatech či kanálech a **1** na fóru [S1]. Stavové značky uváděly **11** schválených či živých, **8** síťových či zpracovatelských chyb, **4** s požadavkem 3DS, **5** zamítnutých a **20** bez označení [S1].

Samostatně odkazovalo na Česko **1 775 nabídkových příspěvků** bez čitelných čísel karet [S1]. V čele stálo **1 570 aktualizací karetních obchodů** (medián **51 zemí** a **1 545 karet** v dávce za **10 až 25 USD**) [S1]. Ani čitelné záznamy, ani oznámení karetních obchodů neověřují platnost karty, průnik u českého vydavatele ani zůstatek; týmy karetních podvodů by měly reagovat výhradně na ověřená upozornění BIN a transakční telemetrii [S1].

8.4 Druhotné škody po potvrzených českých únicích dat

Čtyři potvrzené komerční úniky (**nebankovní dcery skupiny Partners**, **BitFaktura**, **Rohlík.cz** a **Dedoles / `ui42`**) spolu s **Univerzitou Karlovou** ukazují, jak odcizený obchodní kontext živí navazující podvody i při zachování bezpečí hesel a karet [S42][S44][S46][S52][S55]:

- **Fakturace a přesměrování B2B plateb (`BitFaktura`).** Přístup k adresářům dodavatelů, daňovým číslům a historii faktur umožňuje vysoce věrohodné e-maily se změněným IBAN mířené na účetní malých a středních firem [S44][S45].
- **Spotřebitelský smishing se skutečnými objednávkami (`Rohlík.cz` a `Dedoles`).** Šest měsíců přepisů podpory Rohlíku a pět let objednávek Dedolesu umožňuje podvodníkům odkazovat v hovorech a SMS na skutečné dodávky, reklamace či vratky [S46][S47][S55][S56].
- **Napodobování poradců a univerzity (`Partners` a `Univerzita Karlova`).** Zpřístupněné údaje klientů finančního poradenství a studentů usnadňují cílené investiční podvody, falešné portály pro změnu hesla a podvodné odkazy ke stipendiím či poplatkům [S43][S52][S54].

KLÍČOVÉ ZÁVĚRY

01

České bankovní podvody dosáhly 11,8 miliardy Kč v pokusech napříč 75 637 útoky v Q1 až Q3 2026 a březnová policejní čísla stanovila rekord 2 533 případů.

02

Blokování spoofingu ze strany ČTÚ přesunulo podvodníky z pevných linek ke smishingu, falešnému Portálu občana a pronájmu fyzických českých SIM.

03

Po každém zákaznickém či fakturačním úniku okamžitě vydejte jasná varování před napodobováním a zaveďte zpětné kontroly změn IBAN.

KAPITOLA 09

Bankovnictví, silná autentizace a kontinuita plateb

09

TATO KAPITOLA ODPOVÍDÁ

Jak útočníci cílí na Bank iD, české retailové klienty a legalizační účty?

10 z 25

vybraných českých finančních domén mělo 27. listopadu 2026 aktuální nabídku přihlašovacích údajů

9.1 Stav finančního sektoru a expozice licencovaných bank 71

9.2 Poptávka po Bank iD a MojeID, falešný Portál občana a zprostředkovatelé legalizačních účtů 72

9.3 Dohled DORA, hlášení SDAT a provozní odolnost 74

KAPITOLA 09

Bankovnictví, silná autentizace a kontinuita plateb

VE ZKRATCE

Bankovní perimetr je v poštovní hygieně velmi odolný: 23 z 25 finančních domén (13 ze 14 licencovaných bank) vynucuje DMARC a 20 podepisuje DNSSEC. Vnější expozice však ukazuje 10 z 25 finančních domén (7 ze 14 bank) s aktuálními nabídkami údajů. U 13 bank pak 29 729 nezaměstnaneckých zařízení nejpravděpodobněji odráží infikovaná zařízení klientů, vedle phishingu Bank iD a sítí bílých koňů. Nejprve ověřte aktuální nabídky, oddělte firemní a klientské třídění a připravte JSON pro ČNB SDAT od ledna 2027.

9.1 Stav finančního sektoru a expozice licencovaných bank

Napříč **25doménovou skupinou Bankovnictví a finance** (snímek 27. listopadu 2026, všech 25 domén vyhodnoceno) je ochrana perimetru nejsilnější v Česku, zatímco vnější expozice upozorňuje na riziko klientských koncových zařízení [S3][S4][S31]. V celé 25doménové skupině vynucuje DMARC **23 z 25 domén (92 %)** (10 `reject`, 13 `quarantine`, 2 `none`, **0 chybějících**) [S3]. Celkem **25** publikuje SPF, **20** má záznam DKIM, **20** podepisuje DNSSEC DS a **21** vynucuje HSTS [S3]. Na signálech Brandefense Atlas vykázalo **10 z 25** finančních domén aktuální nabídku přihlašovacích údajů [S4]. Celkem **22** domén mělo **nejméně 39 079 vazeb na zařízení** (**299 zaměstnaneckých** u 16 domén; **38 780 ostatních**) a **24** mělo **204 055 historických záznamů hesel** [S4].

Zúžení přísně na **14 licencovaných komerčních bank** uvnitř této skupiny ukazuje koncentraci rizika u klientských zařízení (při zachování jmenovatele 14 bank) [S3][S4]:

Ukazatel (snímek 27. listopadu 2026)	Celá skupina finance (n = 25)	Licencované komerční banky (n = 14)	Provozní závěr	Zdroje
DMARC `reject` / `quarantine`	23 (10 reject, 13 quarantine)	13 (5 reject, 8 quarantine)	Nejsilnější ochrana proti podvržení napříč všemi deseti sektory	[S3]
DMARC `none` / chybí	2 none, 0 chybí	1 none, 0 chybí	Převeďte zbývající monitorovací bankovní domény na quarantine nebo reject	[S3]
SPF / DKIM / DNSSEC DS	25 / 20 / 20	14 / 10 / 12	Široké nasazení kryptografického podepisování DNS a pošty	[S3]
Domény s aktuální nabídkou přístupů	10 domén	7 domén	Ověřte aktivní nabídky do pěti pracovních dnů	[S4]
Nezaměstnanecké vazby na zařízení	38 780 (22 domén)	29 729 (13 domén; top 3 drží 56,3 %)	Primárně koncová zařízení klientů s infostealery, nikoli bankovní servery	[S4]

Ukazatel (snímek 27. listopadu 2026)	Celá skupina finance (n = 25)	Licencované komerční banky (n = 14)	Provozní závěr	Zdroje
Zaměstnanecké vazby na zařízení	299 (16 domén)	200 (9 domén)	Srovnejte se spravovanými stanicemi zaměstnanců a zrušte relace	[S4]
Historické záznamy hesel	204 055 (24 domén)	Nepublikováno	Víceletá kumulativní expozice; nikdy se nerovná průniku roku 2026	[S4]
365denní zmínky domén (chat / web)	2 domény (3) / 0	1 doména (2) / 0	Přímé zmínky domén zůstávají minimální i při vysokém objemu zpráv o bílých koních	[S4]

Počty nezaměstnaneckých zařízení (**29 729** u 13 licencovaných bank, kde první tři banky drží **56,3 %**) nejpravděpodobněji odrážejí infikovaná zařízení retailových klientů spíše než průniky do bankovní infrastruktury [S4]. Pozorované počty platebních karet v §8.3 nestanovují ověřené pořadí českých bank ani průnik u vydavatele [S1].

9.2 Poptávka po Bank iD a MojeID, falešný Portál občana a zprostředkovatelé legalizačních účtů

Zatímco bankovní domény zůstávají klidné, jména českých retailových bank a silné elektronické identity stojí ve středu české podvodné ekonomiky (`Případ G`) [S1][S25][S31][S32].

Karta důkazu B15 12. 8. 2026

Autor v kanálu (přezdívka skryta) Telegramový kanál Telegram Ruština

ORIGINÁL

Помогите пройти верификацию в приложении [Czech consumer app] Для верификацию, нужен чешский bank id 100$ за каждый аккаунт, нужно много.

PŘEKLAD

Pomozte projít ověřením v aplikaci [česká spotřebitelská aplikace]. K ověření je potřeba české Bank iD. 100 USD za každý účet, potřebuji jich hodně.

Poznámka. Kontakty a názvy aplikací jsou odstraněny; přímo odpovídá oficiálním varováním Bank iD a Portálu občana.

Doloženo
Srpnový ruskojazyčný zájemce na Telegramu nabízí 100 USD za účet pro hromadné ověřování přes české Bank iD, vedle srpnové poptávky po ověření českého MojeID (WTB KYC MojeID Only Czech Republic) a únorové poptávky po účtech ověřených přes Bank iD.

Neprokázáno
Dokončené zneužití Bank iD či MojeID, kompromitaci banky ani zapojení konkrétních českých obyvatel.

Karta důkazu B16 15. 1. 2026

Autor v kanálu (přezdívka skryta) Telegramový kanál Telegram Ruština

ORIGINÁL

Словакия Все банки Передача в городе Братислава. Чехия [Czech retail banks] Передача Прага или дистант. Польша [Polish banks] Варшава, Вроцлав Встреча/Передача. Вкусный процент, уточнять в лс.

PŘEKLAD

Slovensko: všechny banky, předání v Bratislavě. Česko: [české retailové banky], předání v Praze nebo na dálku. Polsko: [polské banky], Varšava, Vratislav schůzka či předání. Dobré procento, detaily v soukromé zprávě.

Poznámka. Názvy bank a kontakty jsou odstraněny.

Doloženo
Ruskojazyčný zprostředkovatel na Telegramu inzeruje přeshraniční předávání bankovních účtů bílých koní v Praze, Bratislavě, Varšavě a Vratislavi, vedle lednových až říjnových inzerátů oceňujících české bankovní účty na 170 až 700 USD nebo provizi 20 až 35 %.

Neprokázáno
Kompromitaci systémů jakékoli banky, reálný počet aktivních bílých koní ani ověřený objem transakcí.

Srpnový až říjnový nárůst na Telegramu poháněly dva propojené zločinecké trhy [S1]:

- **Přímá poptávka po české elektronické identitě (B15).** Mezi **10. a 12. srpnem 2026** nabízeli kupci na Telegramu **100 USD za účet české Bank iD**, po dřívější poptávce ze 4. února [S1]. Jiný příspěvek hledal `WTB. KYC MojeID. Only Czech Republic` [S1]. Oficiální varování **Bank iD** (aktualizováno 9. listopadu) a **Portálu veřejné správy** popisují podvodné SMS o vrácení daní či dávkách vedoucí na falešné stránky Portálu občana [S31][S32]. Tyto phishingové weby sbírají přihlašovací údaje Bank iD a navádějí oběti k přeposílání potvrzovacích kódů nebo převodu peněz na „bezpečný účet" [S31][S32]. Ani poptávka, ani phishing nedokládají žádný průnik do infrastruktury Bank iD či MojeID [S31].
- **Průmyslové středoevropské zprostředkování legalizačních účtů (B16).** V roce 2026 vygenerovaly ruskojazyčné a ukrajinskojazyčné telegramové skupiny **28 287 příspěvků o nákupu či pronájmu finančních účtů**, s vrcholem **13 457 jen v říjnu** [S1]. Zprostředkovatelé nabírali české retailové účty (označované Policií ČR jako **legalizační účty**) s předávkami v **Praze, Bratislavě, Varšavě a Vratislavi** [S1][S25]. Inzeráty uváděly **170 až 700 USD za účet** nebo **20 % až 35 % provizi** (konkrétní názvy bank začerněny) [S1]. Okamžité korunové platby přes systém **CERTIS** České národní banky dávají protipodvodným týmům jen minuty na zastavení odlivu prostředků po potvrzení platby oklamaným klientem [S27][S29].

9.3 Dohled DORA, hlášení SDAT a provozní odolnost

Podle evropského nařízení o digitální provozní odolnosti (**DORA**, nařízení `EU 2022/2554`) vykonává **Česká národní banka (ČNB)** dohled nad řízením ICT rizik, dohledem nad dodavateli a hlášením závažných ICT incidentů v českém finančnictví [S27][S28]. Tento mandát pokrývá banky, pojišťovny, platební instituce a tržní infrastrukturu [S27]. ČNB provedla **první dohledové kontroly na místě podle DORA v roce 2025** [S86]. Její výroční hodnocení upozornilo, že nejčastější nedostatky nesouvisely s novými pravidly, nýbrž s kvalitou interních procesů, dokumentace a výkonu kontrol [S86].

Podle článku 5 nařízení Komise v přenesené pravomoci `(EU) 2025/301` podávají finanční subjekty hlášení závažných ICT incidentů ČNB přes portál **SDAT** (`DORAEU01` / `DORAEU02`) [S28][S68]. Lhůty činí **4 hodiny od klasifikace** (nejpozději **24 hodin od zjištění**) pro prvotní hlášení, **72 hodin** pro průběžnou zprávu a **1 měsíc** pro závěrečnou zprávu [S68]. Pro plánování na přelomu let 2026 a 2027 metodika SDAT ČNB potvrzuje, že od **1. ledna 2027 nahradí strukturovaný formát JSON dosavadní excelové šablony** [S28]. Banky by měly automatizovat generování JSON hlášení s předstihem a udržovat bankovní jádro přísně oddělené od nebankovních dcer a externích marketingových či podpůrných dodavatelů [S28][S42].

Srpnové oznámení Partners Banky tuto architektonickou hranici dokládá v praxi [S42]. Když kyberútok zasáhl čtyři přidružené nebankovní dcery skupiny Partners (`Případ L`), oddělené bankovní jádro zůstalo nedotčeno [S42] [S43].

KLÍČOVÉ ZÁVĚRY

01

23 z 25 finančních domén a 13 ze 14 licencovaných českých bank vynucuje DMARC při minimálních zmínkách domén, což tlačí zločince k phishingu na klienty a náboru bílých koňů.

02

Výslovná poptávka po Bank iD (100 USD) a MojeID spolu se zprostředkovateli v Praze, Bratislavě a Varšavě (170–700 USD) přímo souvisí s vlnou bankovních podvodů za 11,8 mld. Kč.

03

Spojte AML detekci legalizačních účtů a ochranu proti napodobování Bank iD s automatizovanou připraveností na lednový přechod DORA SDAT na JSON v roce 2027.

KAPITOLA 10

Regulace, ohlašovací povinnosti a řízení

10

TATO KAPITOLA ODPOVÍDÁ

Který český úřad, portál, spouštěč a zákonná lhůta platí po incidentu?

24 h / 72 h / 30 dní

zákonná posloupnost hlášení podle zákona č. 264/2025 Sb.

10.1 Zákonná mapa Česka pro rok 2026: zákon č. 264/2025 Sb. a dvoukolejný CSIRT 76

10.2 Matice hlášení pro české organizace napříč úřady 76

KAPITOLA 10

Regulace, ohlašovací povinnosti a řízení

VE ZKRATCE

Zákon o kybernetické bezpečnosti č. 264/2025 Sb. (transponující NIS2) nabyl účinnosti 1. listopadu 2025 a rozdělil řešení incidentů mezi NÚKIB (`GovCERT.CZ`) pro režim vyšších povinností a `CSIRT.CZ` sdružení CZ.NIC pro režim nižších povinností podle smlouvy z 24. listopadu 2026. Finanční subjekty hlásí ČNB podle DORA (`lex specialis`), úniky osobních údajů směřují k ÚOOÚ do 72 hodin a od 11. září 2026 platí hlášení výrobců podle článku 14 EU CRA. Ověřte přístupy do portálů a lhůty ještě dnes.

10.1 Zákonná mapa Česka pro rok 2026: zákon č. 264/2025 Sb. a dvoukolejný CSIRT

Zákon č. 264/2025 Sb., o kybernetické bezpečnosti, nabyl účinnosti **1. listopadu 2025**, nahradil zákon č. 181/2014 Sb. a transponoval evropskou směrnici NIS2 do českého práva [S21]. Podle **ustanovení § 6 odst. 1** musejí organizace splňující kritéria ohlásit svou regulovanou službu NÚKIB přes **Portál NÚKIB** do **60 dnů** od splnění podmínek [S21]. Podle **ustanovení § 15 odst. 1–2** zavádí český zákon dvoustupňovou architekturu hlášení incidentů [S21][S24]:

- **Režim vyšších povinností.** Subjekty hlásí incidenty přímo **NÚKIB (`GovCERT.CZ`)** [S21][S24].
- **Režim nižších povinností.** Subjekty hlásí incidenty **Národnímu CERT (`CSIRT.CZ`)**, provozovanému sdružením **CZ.NIC** na základě nové veřejnoprávní smlouvy podepsané s NÚKIB **24. listopadu 2026** [S21][S24].

Podle **ustanovení § 15 odst. 4** mají nově registrované regulované subjekty **roční implementační lhůtu** od doručení rozhodnutí o registraci NÚKIB před plným náběhem bezpečnostních a hlásicích povinností [S21]. Subjekty dříve regulované podle zákona č. 181/2014 Sb. zůstávají povinny nepřetržitě podle **ustanovení § 71 odst. 1** [S21]. Podle **ustanovení § 16 odst. 1 a 3** podávají regulované subjekty **rané varování do 24 hodin** a **ohlášení incidentu do 72 hodin** (nebo **24 hodin** u poskytovatelů služeb vytvářejících důvěru) [S21]. Průběžné zprávy následují na vyžádání a **závěrečná zpráva do 30 dnů** [S21].

Horní hranice správních pokut podle **ustanovení § 59 odst. 4** a **§ 60 odst. 7** dosahují **250 milionů Kč nebo 2 % čistého celosvětového ročního obratu** (podle vyšší částky) [S21]. Toto maximum platí pro režim vyšších povinností, strategické služby či neohlášení [S21]. Pro režim nižších povinností činí strop **175 milionů Kč nebo 1,4 %** a pro vybrané procesní přestupky **100 milionů Kč** [S21]. Podle **ustanovení § 70** platí pro finanční subjekty odvětvová pravidla EU, jako je **DORA**, jako lex specialis, aby nedocházelo k duplicitnímu hlášení ICT incidentů [S21][S27].

10.2 Matice hlášení pro české organizace napříč úřady

Protože jediný ransomwarový útok nebo únik ze SaaS může současně spustit kybernetické, finanční, ochranářské i produktové lhůty, měly by právní a bezpečnostní týmy ověřit všech pět režimů níže (provozní přehled, nikoli právní poradenství):

Režim a český / unijní předpis	Příslušný úřad a portál	Spouštěč	Zákonné lhůty	Horní sankce / zákonná poznámka	Zdroje
Zákon o kybernetické bezpečnosti (NIS2) (`zákon č. 264/2025 Sb.` , §§ 6, 15, 16, 59, 60)	**NÚKIB** (`GovCERT.CZ` , Portál NÚKIB) pro vyšší režim; **CSIRT.CZ** (`CZ.NIC`) pro nižší režim	Významný kybernetický incident zasahující regulovanou službu	**24 h** rané varování; **72 h** ohlášení (**24 h** služby důvěry); **30 dní** závěrečná zpráva	Až **250 mil. Kč / 2 %** (vyšší) nebo **175 mil. Kč / 1,4 %** (nižší); 1letý náběh podle § 15 odst. 4	[S21][S24]
Finanční odolnost (DORA) (`EU 2022/2554` , např. v přenesené pravomoci `2025/301` čl. 5)	**ČNB** přes **SDAT** (`DORAEU01` / `DORAEU02`)	Závažný incident související s ICT u dohlíženého finančního subjektu	**4 h** od klasifikace (max. **24 h** od zjištění); **72 h** průběžná; **1 měsíc** závěrečná	Lex specialis podle § 70 zákona 264/2025; **JSON nahradí Excel od 1. 1. 2027**; kontroly běží	[S21][S27][S28] [S68][S86]
Ochrana osobních údajů (`GDPR` + `zákon č. 110/2019 Sb.` , § 62 odst. 5)	**ÚOOÚ** (Úřad pro ochranu osobních údajů)	Porušení zabezpečení osobních údajů s rizikem pro práva jednotlivců	**72 hodin** od zjištění; bez zbytečného odkladu dotčeným při vysokém riziku	Pokuty GDPR platí pro soukromé správce; **§ 62 odst. 5 upouští od správních pokut GDPR u orgánů veřejné moci** (odlišně od § 63)	[S22][S33]
Bezpečnost produktů (EU CRA) (`nař. (EU) 2024/2847` , čl. 14 a 71)	Určený CSIRT a jednotná platforma ENISA	Aktivně zneužívaná zranitelnost nebo závažný incident v produktech s digitálními prvky	**24 h** rané varování; **72 h** ohlášení; **14 dní** (zranitelnost) nebo **1 měsíc** (incident) závěrečná	**Hlášení dle článku 14 platí od 11. září 2026**; obecné povinnosti CRA platí od **11. prosince 2027**	[S69]
Telekomunikace a trestní hlášení (zákon o elektronických komunikacích; trestní zákoník §§ 230–232)	**ČTÚ** (protispoofing); **Policie ČR / NCOZ** (trestná činnost)	Filtrování podvržených hovorů / telekomunikační incidenty; vydírání, podvod či průnik	Operátorské filtrování průběžně; trestní oznámení ihned při vydírání či podvodu	Zajišťuje řetězec důkazů; podporuje mezinárodní zásahy (např. Operation Eastwood)	[S25][S34][S35] [S85]

Dvě česká specifika vyžadují přímou pozornost vedení. Zaprvé, **ustanovení § 62 odst. 5 zákona č. 110/2019 Sb.** upouští od ukládání správních pokut podle GDPR českým **orgánům veřejné moci a veřejným subjektům** (s využitím čl. 83 odst. 7 GDPR) [S22]. Veřejné subjekty zasažené únikem však i tak mohou čelit povinným hlášením ÚOOÚ, nápravným opatřením, hlášení NÚKIB či CSIRT, policejnímu vyšetřování a vysokým nákladům obnovy [S22][S33].

Zadruhé, **čeští výrobci softwaru, IoT a průmyslových zařízení** vstoupili **11. září 2026** do živých povinností hlášení zranitelností podle **článku 14 Aktu o kybernetické odolnosti EU (CRA)** [S69]. Výrobci musejí podávat 24hodinová raná varování u aktivně zneužívaných chyb více než rok před nabytím plné účinnosti CRA dne **11. prosince 2027** [S69].

KLÍČOVÉ ZÁVĚRY

01

Zákon č. 264/2025 Sb. dělí české hlášení NIS2 mezi NÚKIB (vyšší režim) a CSIRT.CZ sdružení CZ.NIC (nižší režim, smluvně potvrzeno 24. listopadu 2026).

02

Finanční instituce postupují podle DORA [redacted] přes portál SDAT ČNB (přechod na JSON 1. ledna 2027), zatímco výrobci od 11. září 2026 podléhají článku 14 EU CRA.

03

Předem ověřte přístupy do portálů, zástupné pověření a oddělené záznamy zjištění a klasifikace dříve, než incident spustí 4hodinové či 24hodinové lhůty.

KAPITOLA 11

Výhled a podmíněné spouštěče pro rok 2027

11

TATO KAPITOLA ODPOVÍDÁ

Které pozorovatelné spouštěče by měly upravit obranný postoj Česka v roce 2027?

5

podmíněných scénářů navázaných na měřitelné provozní indikátory

KAPITOLA 11

Výhled a podmíněné spouštěče pro rok 2027

VE ZKRATCE

Místo obecných předpovědí by čeští obránci měli navázat změny zdrojů pro rok 2027 na pět ověřitelných spouštěčů. Sledujte doběh roční lhůty zákona č. 264/2025 Sb., rychlé vlny nultých dnů v PHP a CMS, skoky telegramových legalizačních účtů, obecní a středněpodnikový ransomware a internetově dostupné OT jednotky. Spojte každý spouštěč s konkrétní telemetrií, aby eskalace obrany zůstala opřena o důkazy.

Scénář	Pozorovatelný spouštěč ke sledování	Pravděpodobný dopad v Česku	Předem připravená změna obrany	Zdroje
1. Doběh registrační vlny zákona 264/2025	Konec ročních implementačních lhůt (§ 15 odst. 4) nově registrovaných subjektů, plné napojení nižšího režimu do `CSIRT.CZ` a přechod SDAT ČNB na JSON 1. 1. 2027	Vyšší počty hlášených incidentů u NÚKIB a CSIRT.CZ; přísnější dohledové kontroly procesů a smluv dodavatelů	Dokončete registraci, otestujte šablony 24h/72h/30d i 4h DORA JSON a doplňte dodavatelské SLA	[S21][S24][S28][S86]
2. Vlny webových a okrajových nultých dnů pod 48 hodin	Nová kritická varování CISA KEV nebo NÚKIB pro PHP, WordPress, Citrix NetScaler, Zimbra nebo rozšířené VPN a firewally	Rychlé oportunistické skenování a aktivní zneužívání (jako v srpnu `wp2shell` a v říjnu `PHP2Shell` na ČVUT)	Aktivujte předem schválené postupy izolace DMZ, záplatujte do 48 hodin a hledejte webové shelly	[S8][S15][S48][S49] [S64][S79]
3. Eskalace legalizačních účtů a phishingu na Bank iD	Obnovený nárůst nad 10 000 měsíčních příspěvků o finančních účtech na Telegramu, nové smishingové sady Bank iD / Portál občana či růst podvodů s `legalizačními účty`	Vyšší škody retailu a firem navzdory 81% záchytu bank; rychlejší vyvedení korun přes okamžité platby a přeshraniční bílé koně	Zpřísňujte detekci anomálií při zakládání účtů, rozšiřte mimopásmová potvrzení a vydávejte společná varování	[S1][S25][S29][S31] [S32]
4. Přetrvávání obecního a pobočkového ransomwaru	Pokračující regionální aktivita vyděračských označení uvedených v §7.1 proti obcím, pobočkovým sítím a středním dodavatelským řetězcům	Vícedenní či několikatýdenní hotovostní a papírový provoz u méně vybavených obcí a prodejních sítí	Čtvrtletně testujte obnovu ze vzduchově oddělených či páskových záloh, oddělte sítě městské policie a uzavřete obecní mezery v DMARC	[S2][S3][S37][S39] [S41][S57]
5. Průnik vystavených OT a povinností EU CRA	První potvrzený český incident u maloobchodního chlazení či automatizace budov odpovídající evropské vlně, nebo aktivní chyba v českém připojeném produktu	Znehodnocení chlazeného zboží, výpadek vytápění nebo povinná 24hodinová hlášení výrobců podle čl. 14 CRA	Odpojte každou vystavenou jednotku chlazení, HVAC a PLC z veřejného IP prostoru a otestujte příjem hlášení čl. 14 CRA	[S51][S58][S69]

KLÍČOVÉ ZÁVĚRY

01

Berte vypršení ročních lhůt zákona 264/2025 a přechod DORA SDAT na JSON k 1. lednu 2027 jako pevné technické termíny, nikoli papírové milníky.

02

Předem schvalte nouzovou izolaci webových rozhraní, aby příští vlna PHP či CMS nevyvolala zmatená ad-hoc rozhodnutí.

03

Sledujte vlny legalizačních účtů na Telegramu, inventář vystavených OT a testy obnovy z offline záloh jako hlavní včasné indikátory pro rok 2027.

KAPITOLA 12

Akční plán obránců a referenční tabulka nápravy

12

TATO KAPITOLA ODPOVÍDÁ

Kdo jedná jako první, v jakém termínu a s jakým důkazem splnění?

0–90 dní

seřazená cestovní mapa obránců a ověřená tabulka opravených verzí CVE

12.1 Prioritní akční linie a důkazy splnění 83

12.2 Referenční tabulka nápravy zranitelností 85

12.3 Podpora průběžného ověřování 86

KAPITOLA 12

Akční plán obránců a referenční tabulka nápravy

VE ZKRATCE

Záplatování kritických chyb PHP, WordPressu, Citrixu, Office, Zimbry a routerů, izolace vystavených OT jednotek a ověření offline záloh začínají ihned místo čekání na roční audity. Přiřaďte každou níže uvedenou linii jmenovanému technickému vlastníkovi a sponzorovi z vedení a vyžadujte datovaný technický důkaz splnění místo pouhých směrnic.

12.1 Prioritní akční linie a důkazy splnění

1**Ihned (0–7 dní)**

Zmapujte veřejné PHP portály, weby WordPress, brány Citrix NetScaler, servery Zimbra, vystavené VNC, starší routery TP-Link/SOHO a jednotky chlazení/HVAC; nasaďte aktuální verze z §12.2 (nebo vyměňte vyřazený hardware), odpojte OT a VNC z veřejného internetu a předem schvalte nouzové odpojení DMZ

VLASTNÍK

Infrastruktura, web ops, OT inženýring a CISO

DŮKAZ SPLNĚNÍ

Podepsaný registr vnějších aktiv, záznamy verzí, nulový nález VNC/OT a schválený postup izolace

Odstraňte přímé RDP z internetu (`Případ C`), vynuťte MFA odolné proti phishingu na VPN, webmailu, Microsoft 365 a univerzitním či firemním SSO, zablokujte zbytečný Device Code Flow, omezte skripty proti ClickFix a ověřte případnou aktuální nabídku přihlašovacích údajů do pěti pracovních dnů

VLASTNÍK

Správa identit a SOC

DŮKAZ SPLNĚNÍ

Audit firewallu/RDP, export Conditional Access, datovaná uzavření nabídek a záznam politiky stanic

2**30 dní**

Srovnejte zařízení označená jako zaměstnanecká (`24 224` u `168` domén) se spravovanou evidencí firemních stanic, zrušte zasažené relace a směrujte nezaměstnanecké signály (`294 482`) do ochrany klientů před podvody

VLASTNÍK

Koncové stanice, identity a podvody

DŮKAZ SPLNĚNÍ

Srovnaný registr třídění zařízení s datovanými revokacemi či dokumentovaným uzavřením

Uzavřete 71 domén bez vynucujícího DMARC (s prioritou krajské a obecní správy, průmyslu a dopravy), ověřte soulad SPF a DKIM, opravte neplatné TLS certifikáty a zapněte HSTS a CAA na veřejných portálech

VLASTNÍK

Bezpečnost pošty a vlastník domény

DŮKAZ SPLNĚNÍ

Živá kontrola DNS DMARC (`quarantine` / `reject`), TLS a HSTS pro všechny spravované domény

Ověřte registraci podle zákona č. 264/2025 Sb. na Portálu NÚKIB, otestujte hlášení vyššího (`GovCERT.CZ`) či nižšího (`CSIRT.CZ`) režimu, prověřte 72hodinové postupy ÚOOÚ a u výrobců příjem podle čl. 14 CRA; finanční subjekty ověří automatizaci JSON pro ČNB SDAT před 1. lednem 2027

VLASTNÍK

Právní, compliance a CISO

DŮKAZ SPLNĚNÍ

Datovaný test přihlášení do portálů, zástupní pracovníci, testovací výstup JSON a plán lhůt

3**60 dní**

Zkontrolujte přístupy všech IT dodavatelů (ponaučení `ui42`), zrušte spící dodavatelské účty, vymažte odstavené archivy e-shopů a podpory (ponaučení `Dedoles` a `Rohlík.cz`), vynuťte nejnižší oprávnění webových aplikací k centrálním databázím (ponaučení `Univerzita Karlova`) a ověřte oddělení banky od nebankovních dcer (ponaučení `Partners Banka`)

VLASTNÍK

Řízení dodavatelů, aplikační bezpečnost a DPO

DŮKAZ SPLNĚNÍ

Záznam zrušených přístupů, protokol smazání archivů, audit databázových rolí a schéma segmentace

U retailových bank, platebních institucí a e-shopů zpřísněte AML kontroly při zakládání účtů proti padělaným výplatním páskám a nastrčeným firmám, doladťe detekci napodobování Bank iD / Portálu občana a proškolte účetní firem proti změnám IBAN na fakturách (ponaučení `BitFaktura`)

VLASTNÍK

Protipodvodný tým, AML a digitální kanály

DŮKAZ SPLNĚNÍ

Protokol testu pravidel AML, šablony varování klientům a záznam zpětných ověření plateb

4**90 dní**

Proveďte úplné cvičení obnovy z offline záloh a ručního záložního provozu (prodej tužkou a papírem či obecní hotovostní přepážky podle Náměště nad Oslavou, Židlochovic a PRO-DOMA) plus krizové komunikační cvičení oddělující kyberútok od technické závady a hacktivistických tvrzení

VLASTNÍK

Sponzor z vedení, kontinuita a CISO

DŮKAZ SPLNĚNÍ

Datovaný protokol času obnovy, zápis z cvičení offline provozu a schválené krizové šablony

12.2 Referenční tabulka nápravy zranitelností

Následující tabulka shrnuje dotčené a opravené verze z archivovaných záznamů NVD, CVE CNA a výrobců pro kritické zranitelnosti zmiňované v této zprávě. Dřívější historické opravy nenahrazují pozdější kumulativní bezpečnostní vydání na podporovaných větvích:

Produkt a CVE	Dotčené verze	Opravené verze a doporučení výměny	Zdroje
PHP (`CVE-2026-109618` , `CVE-2026-109619` [PHP-P2Shell]; plus samostatné 19. lis `CVE-2026-115560` / `GHSA-658j-r8rw-q6mx`)	Pro `CVE-2026-109618` / `109619` : PHP `8.5` před `8.5.12` , `8.4` před `8.4.27` , `8.3` před `8.3.36` , `8.2` před `8.2.35` a nepodporované `8.1` a starší. Pro `CVE-2026-115560` z 19. listopadu: PHP `8.5` před `8.5.13` , `8.4` před `8.4.28` , `8.3` před `8.3.37` , `8.2` před `8.2.36` (včetně říjnových oprav) a starší nepodporované větve.	Okamžitě přejděte na **vydání z 19. listopadu** `8.5.13` , `8.4.28` , `8.3.37` nebo `8.2.36` (či novější podporovaná vydání / OS LTS backporty) [S64][S65]. Migrujte EOL `8.1` a starší (PHP `8.2` dosáhne konce podpory 31. prosince 2026). Pro `CVE-2026-115560` (zapnutý session upload progress plus nesoulad `session.serialize_handler` za běhu či ve sdíleném úložišti relací) ponechte `session.upload_progress.enabled=0` v `php.ini` / FPM s restartem workerů a sjednoťte serializéry [S65].	[S17][S48][S50][S64][S65] [S74][S75][S76]
WordPress Core (`CVE-2026-63030` , `CVE-2026-60137` [`wp2shell`])	`CVE-2026-63030` : WordPress `6.9.x` před `6.9.5` a `7.0.x` před `7.0.2` . `CVE-2026-60137` : WordPress `6.8.x` před `6.8.6` , `6.9.x` před `6.9.5` a `7.0.x` před `7.0.2` .	Okamžitě aktualizujte na WordPress `6.8.6+` , `6.9.5+` nebo `7.0.2+` (nejnovější podporovanou verzi) [S63] [S77][S78]. Obě CVE jsou v CISA KEV; zkontrolujte šablony a pluginy předávající neošetřený vstup do `WP_Query` `author__not_in` a prověřte zasažené webové kořeny na přítomnost webových shellů a skriptů ClickFix.	[S8][S15][S60][S63][S77] [S78]

Produkt a CVE	Dotčené verze	Opravené verze a doporučení výměny	Zdroje
Citrix NetScaler ADC a Gateway (`CVE-2026-88771` , `CVE-2026-88772` ; nahrazeno 12. lis `CTX697305` / `CVE-2026-120868`)	Pro zářijové nulté dny (`CVE-2026-88771` / `88772`): ADC/Gateway `14.1` před `14.1-73.37` , `13.1` před `13.1-64.23` , `14.1` FIPS před `14.1-73.37` FIPS, `13.1` FIPS/NDcPP před `13.1-37.279` . Pro `CTX697305` z 12. listopadu (`CVE-2026-120868`): podporované větve `14.1` a `13.1` před kumulativními bezpečnostními sestaveními `CTX697305` z 12. listopadu a EOL větve.	Nasaďte aktuální podporovaná sestavení Citrix **z 12. listopadu** `CTX697305` (nebo novější) na standardních, FIPS i NDcPP zařízeních a nezůstávejte na zářijových minimech [S79][S80][S81]. Migrujte EOL zařízení, hledejte perzistenci z doby před záplatou a obměňte relační tajemství a klíče.	[S79][S80][S81]
Microsoft Office (`CVE-2026-21509` , `Operation Neusploit`)	Nezáplatované instalace Microsoft Office zranitelné místním obejitím bezpečnostní funkce přes nedůvěryhodné vstupy (zveřejněno 26. ledna 2026; CISA KEV).	Nasaďte lednové 2026 (a navazující kumulativní) bezpečnostní aktualizace Microsoft Office na všechny stanice Windows a vynuťte Chráněné zobrazení a pravidla ASR [S6][S18][S82].	[S6][S18][S82]
Zimbra Collaboration (ZCS) (`CVE-2025-66376`)	Zimbra Collaboration `10.0` před `10.0.18` a `10.1` před `10.1.13` (uložené XSS v Classic UI přes CSS `@import` v HTML e-mailu; CISA KEV).	Přejděte na nejnovější podporované bezpečnostní vydání `10.1.x` (minimum `10.1.13`) [S83]. Protože větev ZCS `10.0` dosáhla konce podpory 31. prosince 2025, migrujte `10.0` a starší české poštovní servery na podporované verze `10.1.x` .	[S8][S18][S83]
SOHO routery TP-Link (`CVE-2023-50224`)	Starší vyřazené modely TP-Link včetně `TL-WR841N` (nesprávná autentizace `dropbearpwd` ve službě `httpd` ; CISA KEV).	Vyměňte nepodporované EOL SOHO routery za modely s aktivní bezpečnostní podporou výrobce; kde dle TP-Link FAQ 5058 existuje prozatímní firmware, ihned jej nahrajte, vypněte správu z WAN a změňte výchozí hesla [S61][S62][S84].	[S7][S61][S62][S84]

12.3 Podpora průběžného ověřování

Organizace hledající cílený přehled o expozici domén, výstrahách infostealerů, napodobujících doménách a tvrzeních z podsvětí mířících na české značky si mohou vyžádat brífink Brandefense na Žádost o demo Brandefense.

KLÍČOVÉ ZÁVĚRY

01

Okamžitě záplatujte PHP, WordPress, Citrix NetScaler, Office, Zimbru a starší routery podle ověřených verzí v §12.2 a odpojte vystavené VNC a OT z veřejného IP prostoru.

02

Do 30 dnů uzavřete 71 nevynucujících domén DMARC a otestujte postupy zákona 264/2025, CSIRT.CZ a ČNB SDAT JSON.

03

K uzavření 60denních a 90denních milníků vyžadujte datované protokoly obnovy z offline záloh, zrušení přístupů dodavatelů a testy AML.

PŘÍLOHY

Přílohy

A–D

TATO KAPITOLA ODPOVÍDÁ

Příloha A. Metoda, rozsah a vyloučení · Příloha B. Registr důkazů · Příloha C. Zdroje · Příloha D. Slovníček pojmů

86
zdrojů

Příloha A. Metoda, rozsah a vyloučení 89
Příloha B. Registr důkazů 91
Příloha C. Zdroje 92
Příloha D. Slovníček pojmů 97

Příloha A. Metoda, rozsah a vyloučení

Srovnávací země byly vybrány jako příklady výhradně pro poskytnutí kontextu; jejich výběr neznamená žebříček ani politické hodnocení.

A.1 Pozorovací okna a oddělení důkazů

V celé zprávě platí oddělená referenční data, která se nikdy neslučují do jednoho jmenovatele. Hlavní sledované období trvá od **1. ledna do 26. listopadu 2026** (UTC podle času zveřejnění) [S1][S2][S4]. Pokrývá příspěvky z podsvětí (`53 404`), záznamy Ransompedia (`50`), zmínky domén za rok 2026 (`1 334`) a veřejné incidenty [S1] [S2][S4]. Období **12. až 26. listopadu 2026** je zkoumáno samostatně v §5.3 bez promítání do celoročních měr [S1] [S2]. Zahrnuje `1 771` příspěvků, `53` příspěvků na fórech, `3` záznamy Ransompedia a `3` potvrzené veřejné incidenty [S1][S2].

Klouzavé 365denní zmínky domén v dark chatech a na dark webu pokrývají **27. listopadu 2025 až 26. listopadu 2026** [S4]. Pasivní kontroly konfigurace (**250 domén**) zachycují stav k **27. listopadu 2026** a všechny externí úřední, zákonné, NVD a mediální zdroje byly ověřeny **27. listopadu 2026** [S3].

A.2 Populace příspěvků z podsvětí a hranice korpusu

Zaznamenané příspěvky označené pro Česko čítají celkem **53 404** napříč Telegramem (`52 926`), fóry (`428`), Discordem (`25`) a paste servery (`25`) [S1]. Srpen (`6 655`), září (`8 940`) a říjen (`18 965`) tvoří **34 560 příspěvků (64,7 %)** [S1]. Tento vrchol odráží ruskojazyčné a ukrajinskojazyčné chaty obchodující s legalizačními účty a KYC (`13 457` příspěvků jen v říjnu), nikoli průniky do bank [S1]. Listopad je neúplný do 26. listopadu (`3 893` příspěvků, včetně `101` příspěvků na fórech, ne všech cílených na Česko) [S1]. Karty `B01` až `B16` zachycují doslovné zveřejněné úryvky a samy o sobě nedokládají obchod ani průnik [S1].

A.3 Vybrané 250doménové portfolio, expozice Atlas a snímek konfigurace

České doménové portfolio tvoří **250 domén** v deseti vyrovnaných skupinách po 25, vyhodnocených k **27. listopadu 2026** [S3][S4]. Výběr je účelový a nepředstavuje statistické sčítání všech českých subjektů. Publikována je jediná národní souhrnná hodnota Atlas (**48/100**); nikde v této zprávě neuvádíme sektorová, skupinová ani firemní skóre [S4].

Signály expozice portfolia zahrnují aktuální nabídky přihlašovacích údajů (`66` domén, všech 66 s historií, `5 431` záznamů) a kumulativní vazby na zařízení (nejméně `318 706` , z toho `24 224` zaměstnaneckých u `168` domén) [S4]. Dále zahrnují historické záznamy hesel (`180 747 551` , z toho `99,4 %` v Telekomunikacích), vazby na dokumenty (`1 010` u `101` domén) a 30denní podobné názvy (`68 245` u `201` domén) [S4]. Tyto signály se mohou překrývat a nikdy nevyjadřují unikátní osoby, rok 2026 ani potvrzené incidenty [S4].

Publikované kategorie DMARC (`reject` , `quarantine` , `none` , chybějící) zachycují stav DNS politiky, nikoli zaručené pokrytí `pct=100` nebo chování příjemců podle RFC 7489 [S70]. Koncové body TLS (`8` z `250`) a HTTP (`2 3` z `250`), které nebylo možné posoudit, uvádíme jako samostatné počty [S3]. Klouzavé 365denní zmínky domén

pokrývají všech 250 domén (`33` domén a `1 931` zmínek v dark chatech; `16` domén a `230` na dark webu) [S4]. Podmnožina roku 2026 zahrnuje `23` domén a `1 334` zmínek [S4]. Údaje pro licencované komerční banky v §9.1 pokrývají přesnou podmnožinu **14 domén** uvnitř 25doménové skupiny Bankovnictví a finance [S3][S4].

A.4 Záznamy ransomwaru a rozsah platebních karet

Ransompedia zaznamenala do 26. listopadu 2026 celkem **50 záznamů označených pro Česko** u 20 vyděračských označení (oproti 27 za celý rok 2025) [S2]. Dvě opakované položky zanechávají nejvýše 48 různých nárokovaných subjektů; pět položek (čtyři potvrzené veřejné české případy) odpovídá veřejným zprávám, zatímco **45 zůstává neověřených a přísně skrytých** [S2].

> ROZSAH ÚDAJŮ O KARTÁCH
>
> Údaje o platebních kartách popisují omezenou pozorovanou publikační populaci. Neodhadují krádeže českých karet, celostátní ztráty z podvodů ani živou platnost karet.

Zaznamenané příspěvky obsahovaly **42 různých záznamů karet označených pro Česko** (`60` výskytů v `55` příspěvcích, `21` BINů) a **1 775 nabídkových příspěvků** bez čitelných čísel (`1 570` mezinárodních aktualizací karetních obchodů) [S1]. Ani jeden počet neověřuje vydání karty, odcizení ani průnik u vydavatele [S1].

A.5 Pravidla jmenování a výslovná vyloučení

České i přeshraniční organizace jsou jmenovány pouze tehdy, když byly oficiálně potvrzeny a široce publikovány v českých či mezinárodních médiích (`public_names.json`). Veškerá osobní jména (činitelů, ředitelů, mluvčích i zasažených jednotlivců) jsou vynechána. Všech 45 neověřených položek Ransompedia je skryto bez párování dat, sektorů a označení. Všechny neověřené cíle z fór či Telegramu i soukromé domény portfolia zůstávají skryty. Čtyři výrazné položky byly z počtů českých kyberincidentů roku 2026 výslovně vyloučeny:

1. **Výpadek ministerstev 13. listopadu 2026.** Zasáhl ministerstva financí, dopravy a školství ve stejný den jako únik SIS Univerzity Karlovy; Microsoft Česko potvrdil nekybernetickou interní technickou poruchu [S54].
2. **Historický průnik APT31 do MZV z let 2022 až 2024.** Veřejně připsán v květnu 2025; citován výhradně jako výchozí kontext před rokem 2026 ze Zprávy NÚKIB za rok 2025 [S5].
3. **Neověřená tvrzení hacktivistů o kamerách a regulaci vytápění.** Tvrzení `Z-Pentest Alliance` a spřízněných kanálů (leden, květen, říjen) nebyla potvrzena nezávislými českými médii ani technickými prověrkami [S1][S58].
4. **Srpnová až říjnová vlna zprostředkování legalizačních účtů na Telegramu.** Šablonový nábor bílých koňů napříč zeměmi (`34 560` příspěvků v srpnu až říjnu) odráží podvodné kanály, nikoli průniky do českých bank [S1].

Příloha B. Registr důkazů

Doslovné úryvky jsou zobrazeny přímo v níže uvedených kapitolách. Data příspěvků vyjadřují čas zveřejnění; žádná karta sama o sobě nedokládá dokončený obchod ani potvrzený průnik.

Karta	Datum	Prostředí	Přezdívka	Jazyk	Kapitola
B01	2026-02-18	Vlákno na fóru	Přezdívka skryta	Angličtina	§4
B02	2026-02-24	Vlákno na fóru	Přezdívka skryta	Angličtina	§4
B03	2026-01-29	Kanál Telegram	Přezdívka skryta	Ruština	§4
B04	2026-04-14	Vlákno na fóru	Přezdívka skryta	Angličtina	§4
B05	2026-01-24	Vlákno na fóru	Přezdívka skryta	Angličtina	§4
B06	2026-05-15	Vlákno na fóru	Přezdívka skryta	Angličtina	§4
B07	2026-03-02	Vlákno na fóru	Přezdívka skryta	Angličtina	§4
B08	2026-07-23	Vlákno na fóru	Přezdívka skryta	Angličtina	§4
B09	2026-11-21	Vlákno na fóru	Přezdívka skryta	Ruština	§4
B10	2026-08-21	Vlákno na fóru	Přezdívka skryta	Angličtina	§8
B11	2026-08-19	Vlákno na fóru	Přezdívka skryta	Angličtina	§8
B12	2026-01-12	Vlákno na fóru	Přezdívka skryta	Ruština	§8
B13	2026-11-22	Vlákno na fóru	Přezdívka skryta	Angličtina	§4
B14	2026-11-19	Vlákno na fóru	Přezdívka skryta	Angličtina	§4
B15	2026-08-12	Kanál Telegram	Přezdívka skryta	Ruština	§9
B16	2026-01-15	Kanál Telegram	Přezdívka skryta	Ruština	§9

Příloha C. Zdroje

S1: Odin by Brandefense. Pozorování z podsvětí a počty příspěvků (1. ledna až 26. listopadu 2026; nedávné okno 12. až 26. listopadu 2026). Ověřeno dne 2026-11-27.

S2: Ransompedia. Záznamy o ransomwaru označené podle zemí (1. ledna až 26. listopadu 2026 a celý rok 2025). Ověřeno dne 2026-11-27.

S3: Odin by Brandefense. Snímek konfigurace 250 vybraných českých domén (27. listopadu 2026). Ověřeno dne 2026-11-27.

S4: Odin by Brandefense. Pozorování expozice Brandefense Atlas u 250 hodnocených českých domén (27. listopadu 2026) a klouzavé 365denní zmínky domén (27. listopadu 2025 až 26. listopadu 2026). Ověřeno dne 2026-11-27.

S5: NÚKIB. 2025 Report on the State of Cybersecurity in the Czech Republic (published August 2026). https://nukib.gov.cz/download/publications_en/2025-Report-on-the-State-of-Cybersecurity-in-the-Czech-Republic.pdf Ověřeno dne 2026-11-27.

S6: NÚKIB. NÚKIB Quarterly: Cyber Threat Landscape Q1/2026. https://nukib.gov.cz/download/publications_en/NUKIB-Quarterly-Q12026.pdf Ověřeno dne 2026-11-27.

S7: NÚKIB. NÚKIB Quarterly: Cyber Threat Landscape Q2/2026. https://nukib.gov.cz/download/publications_en/NUKIB%20Quarterly_Q2_2026.pdf Ověřeno dne 2026-11-27.

S8: NÚKIB. Quarterly Threat Overview Q3 2026 (Čtvrtletní přehled hrozeb pohledem NÚKIB - Q3 2026). https://nukib.gov.cz/download/publikace/vyzkum/Ctvrtletni-prehled-hrozeb-pohledem-NUKIB-Q3-2026.pdf Ověřeno dne 2026-11-27.

S9: NÚKIB. Monthly Cyber Incidents Overview: January 2026 PDF. https://nukib.gov.cz/download/publikace/vyzkum/Kyberneticke-incidenty-pohledem-NUKIB-leden-2026.pdf Ověřeno dne 2026-11-27.

S10: NÚKIB. Monthly Cyber Incidents Overview: February 2026 PDF. https://nukib.gov.cz/download/publikace/vyzkum/Kyberneticke-incidenty-pohledem-NUKIB-unor-2026.pdf Ověřeno dne 2026-11-27.

S11: NÚKIB. Monthly Cyber Incidents Overview: March 2026 PDF. https://nukib.gov.cz/download/publikace/vyzkum/Kyberneticke-incidenty-pohledem-NUKIB-brezen2026.pdf Ověřeno dne 2026-11-27.

S12: NÚKIB. Monthly Cyber Incidents Overview: April 2026 PDF. https://nukib.gov.cz/download/publikace/vyzkum/Kyberneticke-incidenty-pohledem-NUKIB-duben-2026.pdf Ověřeno dne 2026-11-27.

S13: NÚKIB. Monthly Cyber Incidents Overview: June 2026 PDF. https://nukib.gov.cz/download/publikace/vyzkum/Kyberneticke-incidenty-pohledem-NUKIB-cerven-2026.pdf Ověřeno dne 2026-11-27.

S14: NÚKIB. Monthly Cyber Incidents Overview: July 2026 PDF. https://nukib.gov.cz/download/publikace/vyzkum/Kyberneticke-incidenty-pohledem-NUKIB-cervenec-2026.pdf Ověřeno dne 2026-11-27.

S15: NÚKIB. Monthly Cyber Incidents Overview: August 2026 PDF. https://nukib.gov.cz/download/publikace/vyzkum/Kyberneticke-incidenty-pohledem-NUKIB-srpen-2026.pdf Ověřeno dne 2026-11-27.

S16: NÚKIB. Monthly Cyber Incidents Overview: September 2026 PDF. https://nukib.gov.cz/download/publikace/vyzkum/Kyberneticke-incidenty-pohledem-NUKIB-zari-2026.pdf Ověřeno dne 2026-11-27.

S17: NÚKIB. Monthly Cyber Incidents Overview: October 2026 PDF. https://nukib.gov.cz/download/publikace/vyzkum/Kyberneticke-incidenty-pohledem-NUKIB-rijen-2026.pdf Ověřeno dne 2026-11-27.

S18: NÚKIB. Threat Analysis (20 October 2026): Russian State-Sponsored Actors Exploit Vulnerabilities and Users' Lack of Vigilance. https://nukib.gov.cz/download/publications_en/Russian-State-sponsored-Actors-Exploit-Vulnerabilities-and-Users-Lack-of-Vigilance.pdf Ověřeno dne 2026-11-27.

S19: NÚKIB. Joint international warning on pro-Russian hacktivist groups attacking critical infrastructure (11 December 2025). https://nukib.gov.cz/en/infoservis-en/news/2357-the-nukib-has-joined-an-international-warning-about-pro-russian-hacktivist-groups-attacking-critical-infrastructure-entities/ Ověřeno dne 2026-11-27.

S20: NÚKIB. Approval of the National Cyber Security Strategy of the Czech Republic (8 September 2025). https://nukib.gov.cz/cs/infoservis/aktuality/2300-vlada-ceske-republiky-schvalila-novou-narodni-strategii-kyberneticke-bezpecnosti-ceske-republiky/ Ověřeno dne 2026-11-27.

S21: Zákony pro lidi. Act No. 264/2025 Coll., on Cybersecurity (effective 1 November 2025). https://www.zakonyprolidi.cz/cs/2025-264 Ověřeno dne 2026-11-27.

S22: Zákony pro lidi. Act No. 110/2019 Coll., on Personal Data Processing. https://www.zakonyprolidi.cz/cs/2019-110 Ověřeno dne 2026-11-27.

S23: CZ.NIC / CSIRT.CZ. CSIRT.CZ Annual Report 2025 press release (31 March 2026; 3,005 incidents). https://www.nic.cz/cs/o-nas/aktuality/novinky/4631-bezpecnostni-tym-csirtcz-vydal-vyrocni-zpravu-za-rok-2025/ Ověřeno dne 2026-11-27.

S24: CSIRT.CZ (CZ.NIC). Public-law contract confirming CZ.NIC continues operating National CSIRT under Act 264/2025 Coll. (24 November 2026). https://csirt.cz/cs/o-nas/novinky/cz-nic-bude-nadale-provozovat-narodni-csirt/ Ověřeno dne 2026-11-27.

S25: Ministry of the Interior (MV ČR). Report on the Internal Security and Public Order Situation in the Czech Republic in 2025 (21,137 cybercrimes, +14.3% YoY). https://mv.gov.cz/documents/zprava-o-situaci-v-oblasti-vnitrni-bezpecnosti-a-verejneho-poradku-na-uzemi-cr-v-roce-2025 Ověřeno dne 2026-11-27.

S26: Novinky.cz (ČTK / Police of the Czech Republic). Record March 2026 cybercrime surge: 2,533 cases (+37% YoY) and vishing losses (15 April 2026). https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-narust-kyberkriminality-v-cesku-je-rekordni-bije-na-poplach-policie-40573402?noredirect=1 Ověřeno dne 2026-11-27.

S27: Czech National Bank (ČNB). DORA supervisory overview (Digital Operational Resilience Act). https://www.cnb.cz/cs/dohled-financni-trh/dora-digitalni-provozni-odolnost-financniho-trhu/ Ověřeno dne 2026-11-27.

S28: Czech National Bank (ČNB). DORA reporting methodology and SDAT framework (DORAEU01 / DORAEU02). https://www.cnb.cz/cs/statistika/metodicke-informace/dora/ Ověřeno dne 2026-11-27.

S29: Radio Prague International (Český rozhlas / ČBA). Q1-Q3 2026 Czech banking cyber-fraud report: CZK 2.2B lost, CZK 9.6B protected, 75,637 attacks (10 November 2026). https://cesky.radio.cz/cba-skoda-klientu-bank-z-kyberpodvodu-stoupla-letos-o-polovinu-na-22-mld-kc-8902211 Ověřeno dne 2026-11-27.

S30: Banky.cz (ČBA / Ipsos). Q1-Q3 2026 banking cyber-fraud breakdown and Cybersecurity Index (12 November 2026). https://www.banky.cz/clanky/kyberpodvody-2026-skody-pres-22-mld-kc-pri-vice-nez-75-tisicich-utocich/ Ověřeno dne 2026-11-27.

S31: Bank iD (bankid.cz). Official fraud warning on Bank iD impersonation and safe-account scams (9 November 2026). https://bankid.cz/clanky/jak-poznat-podvod/ Ověřeno dne 2026-11-27.

S32: Portál veřejné správy (portal.gov.cz / DIA). Official warning on fraudulent SMS, emails and fake Portál občana / Bank iD login portals. https://portal.gov.cz/kam-dal/pozor-na-podvodne-sms-a-emaily Ověřeno dne 2026-11-27.

S33: Ochrana údajů (ochranaudaju.cz). Summary of ÚOOÚ 2025 Annual Report: 392 breach notifications and 3,854 submissions (20 March 2026). https://www.ochranaudaju.cz/aktuality/vyrocni-zprava-uoou-za-rok-2025 Ověřeno dne 2026-11-27.

S34: Lupa.cz. ČTÚ evaluation of anti-spoofing regulation and rising SMS phishing (29 November 2024). https://www.lupa.cz/aktuality/opatreni-proti-spoofingu-splnila-ucel-pochvaluje-si-ctu/ Ověřeno dne 2026-11-27.

S35: Novinky.cz. Electronic Communications Act amendment against spoofed foreign calls (5 March 2025). https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-podvodnych-telefonatu-jsou-miliony-mesicne-operatori-proti-nim-budou-mit-novou-zbran-40510979?noredirect=1 Ověřeno dne 2026-11-27.

S36: Government of the Czech Republic (vlada.gov.cz). State Security Council statement on the Czech ammunition initiative (7 January 2026). https://vlada.gov.cz/cz/media-centrum/aktualne/bezpecnostni-rada-statu-se-zabyvala-ceskou-municni-iniciativou-224703/ Ověřeno dne 2026-11-27.

S37: Novinky.cz. Ransomware attack on Městský úřad Jemnice (10 March 2026). https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-urad-na-trebicsku-ochromil-ransomware-kybersmejdi-chteji-vykupne-40566928?noredirect=1 Ověřeno dne 2026-11-27.

S38: Novinky.cz. Deadlock ransomware attack on Městský úřad Židlochovice (17 March 2026). https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-zasifruje-data-a-pozaduje-vykupne-za-odemknuti-radnici-v-zidlochovicich-napadl-vyderacsky-virus-40568203?noredirect=1 Ověřeno dne 2026-11-27.

S39: Seznam Zprávy. Month-later recovery report on Městský úřad Židlochovice cyberattack (16 April 2026). https://www.seznamzpravy.cz/clanek/domaci-zivot-v-cesku-urednici-doma-platby-jen-v-hotovosti-hackersky-utok-suzuje-mesto-u-brna-304125?noredirect=1 Ověřeno dne 2026-11-27.

S40: Novinky.cz (ČTK). Cyberattack and offline-backup restoration at Městský úřad Náměšť nad Oslavou (1 April 2026). https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-hackeri-ochromili-mestsky-urad-na-trebicsku-40570997?noredirect=1 Ověřeno dne 2026-11-27.

S41: Novinky.cz. Police criminal investigation into cyberattack on Městský úřad Šumperk (July 2026). https://www.novinky.cz/clanek/krimi-policie-zahajila-setreni-kybernetickeho-utoku-na-sumperk-pachatelum-hrozi-ctyri-roky-vezeni-40590244?noredirect=1 Ověřeno dne 2026-11-27.

S42: Partners Banka (partnersbanka.cz). Official notice on Partners Group security incident confirming Partners Banka unaffected (27-31 August 2026). https://www.partnersbanka.cz/partners-bezpecnostni-incident Ověřeno dne 2026-11-27.

S43: Novinky.cz. Partners Group cyberattack and client personal-data breach (27 August 2026). https://www.novinky.cz/clanek/ekonomika-partners-bance-po-hackerskem-utoku-unikly-osobni-udaje-klientu-40594788?noredirect=1 Ověřeno dne 2026-11-27.

S44: BitFaktura (bitfaktura.cz). Official security-incident notice and remediation timeline (29 September - 6 October 2026). https://bitfaktura.cz/bezpecnostni-incident Ověřeno dne 2026-11-27.

S45: Seznam Zprávy. BitFaktura invoicing database breach reporting (October 2026). https://www.seznamzpravy.cz/clanek/ekonomika-firmy-z-fakturacni-sluzby-bitfaktura-unikla-data-hrozi-utoky-varuje-firma-317013?noredirect=1 Ověřeno dne 2026-11-27.

S46: Lupa.cz. Rohlík.cz customer-support tool data breach (11 October 2026). https://www.lupa.cz/aktuality/rohliku-unikla-data-o-zakaznicich-utocnik-mohl-videt-jejich-adresy-telefony-i-konverzace-s-ai/ Ověřeno dne 2026-11-27.

S47: Seznam Zprávy. Rohlík.cz customer-support breach and secondary-fraud warnings (12 October 2026). https://www.seznamzpravy.cz/clanek/ekonomika-firmy-chleba-nebo-vino-hackeri-vi-o-nakupech-na-rohliku-a-mohou-to-pouzit-k-podvodum-317648?noredirect=1 Ověřeno dne 2026-11-27.

S48: ČT24 (ČTK / Reuters). NÚKIB PHP2Shell advisory and precautionary shutdown of Úřad vlády ČR and ČHMÚ websites (21 October 2026). https://ct24.ceskatelevize.cz/clanek/svet/vlady-odstavuji-weby-kvuli-bezpecnostnim-chybam-v-programovacim-jazyku-php-378877 Ověřeno dne 2026-11-27.

S49: ČT24 (ČTK). Cyberattack on ČVUT linked to global PHP vulnerability wave (22 October 2026). https://ct24.ceskatelevize.cz/clanek/domaci/hackeri-zautocili-na-cvut-univerzita-odstavila-cast-systemu-378916 Ověřeno dne 2026-11-27.

S50: Lupa.cz. PHP2Shell critical vulnerabilities analysis and Czech public-sector response (21 October 2026). https://www.lupa.cz/aktuality/php2shell-kriticke-zranitelnosti-v-php-davaji-utocnikum-moznost-spustit-kod-na-serverech/ Ověřeno dne 2026-11-27.

S51: ČT24 (ČTK / NÚKIB). European refrigeration-controller cyberattacks and NÚKIB preventive guidance (11 November 2026). https://ct24.ceskatelevize.cz/clanek/domaci/evropa-celi-kyberutokum-na-chladici-zarizeni-nukib-doporucuje-preventivni-opatreni-379438 Ověřeno dne 2026-11-27.

S52: Univerzita Karlova (cuni.cz). Official statement on Student Information System (SIS) cybersecurity incident (UK-16212, 13 November 2026). https://cuni.cz/UK-16212.html Ověřeno dne 2026-11-27.

S53: Univerzita Karlova (cuni.cz). Official follow-up statement confirming no widespread CAS account compromise (UK-16214, November 2026). https://cuni.cz/UK-16214.html Ověřeno dne 2026-11-27.

S54: ČT24 (ČTK). Charles University CAS preventive password reset and Microsoft Czechia non-cyber outage confirmation (14 November 2026). https://ct24.ceskatelevize.cz/clanek/domaci/kyberutok-plosne-neohrozil-uzivatelske-ucty-uvedla-univerzita-karlova-379616 Ověřeno dne 2026-11-27.

S55: Lupa.cz. Dedoles legacy e-shop data breach via Slovak IT supplier ui42 (23 November 2026). https://www.lupa.cz/aktuality/z-dalsi-zname-znacky-ceske-e-commerce-unikla-data-zakazniku-utok-zasahl-dedoles/ Ověřeno dne 2026-11-27.

S56: Živé.sk (Aktuality.sk). Dedoles legacy e-shop customer data breach scope (20 November 2026). https://zive.aktuality.sk/clanok/GoM25C9/dedoles-priznal-uspesny-kyberutok-ake-udaje-zakaznikov-ziskali-hackeri/ Ověřeno dne 2026-11-27.

S57: Seznam Zprávy. PRO-DOMA building-materials ransomware attack, tape backups and infrastructure rebuild (25 November 2026). https://www.seznamzpravy.cz/clanek/ekonomika-firmy-stavebniny-pro-doma-se-staly-cilem-kybernetickeho-utoku-omezily-provoz-321533?noredirect=1 Ověřeno dne 2026-11-27.

S58: Lupa.cz. Unverified hacktivist camera and heating-control claims: Check Point and BIS context (9 October 2026). https://www.lupa.cz/aktuality/rusti-hackeri-tvrdi-ze-v-cr-ovladli-tisice-bezpecnostnich-kamer-napadli-pry-i-rizeni-vytapeni/ Ověřeno dne 2026-11-27.

S59: ESET Czechia. Ransomware in Czechia Q1 2026 press release: 100% YoY increase, Gentlemen, Akira and Qilin (1 April 2026). https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/ransomware-vcesku-100procentni-narust-utoku-tri-svetove-gangy-a-nova-era-sofistikovanych-hrozeb/ Ověřeno dne 2026-11-27.

S60: ESET Czechia. Q3 2026 macOS threats: ClickFix delivery and PSW.Agent infostealer in Czechia and Slovakia (4 November 2026). https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/hrozby-pro-macos-v-utocich-na-pocitace-od-apple-prevlada-technika-clickfix-pomaha-sirit-infostealer/ Ověřeno dne 2026-11-27.

S61: FBI IC3. PSA260407: Russian GRU exploiting vulnerable routers to steal sensitive information (7 April 2026). https://www.ic3.gov/PSA/2026/PSA260407 Ověřeno dne 2026-11-27.

S62: TP-Link. Security Advisory for CVE-2023-50224: Impact on Legacy Router Products (FAQ 5058). https://www.tp-link.com/en/support/faq/5058/ Ověřeno dne 2026-11-27.

S63: F5 Labs. CVE-2026-63030 and CVE-2026-60137 (wp2shell): captured exploit payload and remediation. https://www.f5.com/labs/articles/cve-2026-63030-and-cve-2026-60137-wp2shell-captured-exploit-payload Ověřeno dne 2026-11-27.

S64: PHP Project. 2026 security releases archive (October and November 2026 fixes). https://www.php.net/archive/2026.php Ověřeno dne 2026-11-27.

S65: PHP Project (GitHub Security Advisory). GHSA-658j-r8rw-q6mx: Session serializer mismatch remote code execution (CVE-2026-115560, 19 November 2026). https://github.com/php/php-src/security/advisories/GHSA-658j-r8rw-q6mx Ověřeno dne 2026-11-27.

S66: DataReportal. Digital 2026: Czechia (9.96 million internet users, 94.2% penetration). https://datareportal.com/reports/digital-2026-czechia Ověřeno dne 2026-11-27.

S67: ČT24. 2026 Czech civic and institutional calendar (cabinet confidence vote and October municipal/Senate elections; 31 December 2025). https://ct24.ceskatelevize.cz/clanek/domaci/rok-2026-v-cesku-nova-vlada-obecni-volby-i-zmeny-v-zapisech-prvnacku-368603 Ověřeno dne 2026-11-27.

S68: European Commission (EU Publications Office / Cellar). Commission Delegated Regulation (EU) 2025/301, Article 5 (DORA major ICT incident reporting time limits). https://publications.europa.eu/resource/cellar/36795cde-ef2b-11ef-981b-01aa75ed71a1.0006.03/DOC_1 Ověřeno dne 2026-11-27.

S69: European Parliament and Council (EU Publications Office / Cellar). Regulation (EU) 2024/2847 (Cyber Resilience Act), Articles 14 and 71. https://publications.europa.eu/resource/cellar/21b7d4eb-a6e2-11ef-85f0-01aa75ed71a1.0006.03/DOC_1 Ověřeno dne 2026-11-27.

S70: RFC Editor. DMARC protocol reference (RFC 7489, March 2015). https://www.rfc-editor.org/rfc/rfc7489.html Ověřeno dne 2026-11-27.

S71: RFC Editor. SPF protocol reference (RFC 7208, April 2014). https://www.rfc-editor.org/rfc/rfc7208.html Ověřeno dne 2026-11-27.

S72: RFC Editor. DKIM signatures reference (RFC 6376, September 2011). https://www.rfc-editor.org/rfc/rfc6376.html Ověřeno dne 2026-11-27.

S73: RFC Editor. HTTP Strict Transport Security reference (RFC 6797, November 2012). https://www.rfc-editor.org/rfc/rfc6797.html Ověřeno dne 2026-11-27.

S74: NVD. CVE-2026-109618 (PHP out-of-memory request cleanup, published 21 October 2026). https://nvd.nist.gov/vuln/detail/CVE-2026-109618 Ověřeno dne 2026-11-27.

S75: NVD. CVE-2026-109619 (PHP global-state use-after-free, published 21 October 2026). https://nvd.nist.gov/vuln/detail/CVE-2026-109619 Ověřeno dne 2026-11-27.

S76: NVD. CVE-2026-115560 (PHP session upload progress serializer mismatch, published 19 November 2026). https://nvd.nist.gov/vuln/detail/CVE-2026-115560 Ověřeno dne 2026-11-27.

S77: NVD. CVE-2026-63030 (WordPress REST API batch route confusion / wp2shell, published 17 July 2026). https://nvd.nist.gov/vuln/detail/CVE-2026-63030 Ověřeno dne 2026-11-27.

S78: NVD. CVE-2026-60137 (WordPress WP_Query SQL injection / wp2shell, published 17 July 2026). https://nvd.nist.gov/vuln/detail/CVE-2026-60137 Ověřeno dne 2026-11-27.

S79: NVD. CVE-2026-88771 (Citrix NetScaler ADC and Gateway improper input validation, published 27 September 2026). https://nvd.nist.gov/vuln/detail/CVE-2026-88771 Ověřeno dne 2026-11-27.

S80: NVD. CVE-2026-88772 (Citrix NetScaler ADC and Gateway RCE/DoS, published 27 September 2026). https://nvd.nist.gov/vuln/detail/CVE-2026-88772 Ověřeno dne 2026-11-27.

S81: NVD. CVE-2026-120868 (Citrix NetScaler ADC and Gateway packet-processing memory overflow, published 12-13 November 2026). https://nvd.nist.gov/vuln/detail/CVE-2026-120868 Ověřeno dne 2026-11-27.

S82: NVD. CVE-2026-21509 (Microsoft Office security feature bypass / Operation Neusploit, published 26 January 2026). https://nvd.nist.gov/vuln/detail/CVE-2026-21509 Ověřeno dne 2026-11-27.

S83: NVD. CVE-2025-66376 (Zimbra Collaboration Classic UI stored XSS, published 5 January 2026). https://nvd.nist.gov/vuln/detail/CVE-2025-66376 Ověřeno dne 2026-11-27.

S84: NVD. CVE-2023-50224 (TP-Link TL-WR841N improper authentication, published 3 May 2024). https://nvd.nist.gov/vuln/detail/CVE-2023-50224 Ověřeno dne 2026-11-27.

S85: ČT24. Europol and Eurojust Operation Eastwood disruption of NoName057(16) (July 2025). https://ct24.ceskatelevize.cz/clanek/svet/europol-a-eurojust-oznamily-ze-rozbily-proruskou-hackerskou-skupinu-363034 Ověřeno dne 2026-11-27.

S86: Právní prostor. ČNB 2025 supervisory review: first on-site DORA inspections in Czechia. https://www.pravniprostor.cz/clanky/financni-pravo/cim-se-zabyvala-cnb-v-roce-2025-prvni-kontroly-podle-dora-a-245-zadosti-o-kryptolicenci Ověřeno dne 2026-11-27.

Příloha D. Slovníček pojmů

- **Národní souhrnná hodnota Atlas.** Jediná hodnota vnější expozice Brandefense Atlas na škále 0 až 100 publikovaná za celé hodnocené portfolio jako celek [S4]. Vyšší číslo značí větší pozorovanou vnější expozici a nikdy nevyjadřuje procento průniků ani pořadí sektorů [S4].
- **Zákon č. 264/2025 Sb. (o kybernetické bezpečnosti).** Český zákon transponující unijní směrnici NIS2, účinný od 1. listopadu 2025, zavádějící režim vyšších a nižších povinností a lhůty 24 h / 72 h / 30 dní [S21].
- **Bank iD.** Český systém elektronické identity vydávané bankami, umožňující občanům přihlašování na Portál občana, veřejné služby i komerční portály pomocí bankovních údajů [S31].
- **BIN (identifikační číslo banky).** Úvodních šest číslic čísla platební karty určujících karetní síť a vydávající instituci [S1].
- **CERTIS.** Mezibankovní platební systém České národní banky zpracovávající korunové platby v reálném čase [S27].
- **ClickFix.** Technika sociálního inženýrství navádějící oběti ke zkopírování a spuštění škodlivých příkazů z falešných ověřovacích či chybových oken [S60].
- **CSIRT.CZ.** Český národní tým CSIRT provozovaný sdružením CZ.NIC, určený k řešení incidentů v režimu nižších povinností podle zákona č. 264/2025 Sb. a smlouvy z 24. listopadu 2026 [S23][S24].
- **DMARC / SPF / DKIM.** Standardy autentizace e-mailu určující oprávněné odesílací servery (SPF), kryptografické podpisy (DKIM) a politiku nakládání s neshodnou poštou (DMARC) [S70][S71][S72].
- **DNSSEC.** Kryptografické podepisování záznamů DNS (doložené záznamy DS v nadřazené zóně) chránící překlad domén proti podvržení [S3].
- **DORA / SDAT.** Nařízení EU o digitální provozní odolnosti (`EU 2022/2554`) a portál SDAT České národní banky (`DORAEU01` / `DORAEU02`) pro hlášení závažných finančních ICT incidentů [S27][S28][S68].
- **EU CRA (Akt o kybernetické odolnosti).** Nařízení `(EU) 2024/2847` zavádějící od 11. září 2026 povinné 24hodinové hlášení výrobců u aktivně zneužívaných zranitelností v připojených produktech [S69].
- **HSTS.** Hlavička HTTP Strict Transport Security přikazující prohlížečům připojovat se výhradně šifrovaně přes HTTPS [S73].
- **KYC (Poznej svého klienta).** Ověřování totožnosti a hloubková kontrola klienta vyžadovaná před založením bankovního, platebního či krypto účtu [S1].
- **Legalizační účty (účty bílých koňů).** Retailové bankovní účty nabírané, kupované či pronajímané zprostředkovateli podvodů k přijímání a rychlému přeposílání odcizených prostředků [S1][S25].
- **MojeID.** Národní služba digitální identity provozovaná sdružením CZ.NIC podporující přístup občanů k českým veřejným i komerčním portálům [S1].
- **NÚKIB (`GovCERT.CZ`).** Národní úřad pro kybernetickou a informační bezpečnost, dohlížející na subjekty v režimu vyšších povinností a provozující Vládní CERT [S5][S21].
- **PHP2Shell / `wp2shell`.** Veřejná označení kritických řetězců zranitelností vzdáleného spuštění kódu roku 2026 v PHP (`CVE-2026-109618`, `CVE-2026-109619`) a jádru WordPressu (`CVE-2026-63030`, `CVE-2026-60137`) [S63] [S74][S75][S77][S78].

- **Portál občana.** Ústřední český online portál propojující obyvatele s daňovými, rejstříkovými a státními elektronickými službami, často napodobovaný při phishingu na Bank iD [S32].
- **TLP:CLEAR.** Označení protokolu Traffic Light Protocol umožňující neomezené veřejné sdílení při dodržení ochrany soukromí a právních povinností.
- **ÚOOÚ.** Úřad pro ochranu osobních údajů, český dozorový úřad pro oblast GDPR [S22][S33].

O této zprávě

Zprávu připravil tým Odin by Brandefense. Verze 1.0 pracuje s oddělenými referenčními daty. Sledované období roku 2026 trvá od 1. ledna do 26. listopadu 2026 (přičemž období 12. až 26. listopadu je hodnoceno zvlášť), zatímco klouzavé 365denní zmínky domén pokrývají 27. listopadu 2025 až 26. listopadu 2026. Hodnocení expozice Brandefense Atlas i pasivní kontroly konfigurace u všech 250 vybraných domén zachycují stav k 27. listopadu 2026. Všechny veřejné zdroje byly ověřeny 27. listopadu 2026.

Tato česká verze překládá anglický originál; v případě rozdílného znění má přednost anglická verze. Doporučení vyžadují ověření podle vlastních aktiv, závislostí služeb a právních povinností každé organizace.

© 2026 Brandefense. Všechna práva vyhrazena.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS

4.7 / 5

COVERAGE

3 pillars

CTI, DRPS, EASM

MONITORING

24 / 7

Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO