BRANDEFENSE COUNTRY REPORT · CZECHIA 2026

Brandefense Czechia Cyber Threat Landscape Report 2026

Municipal ransomware, edge zero-days, supplier breaches and mule-account networks across Czechia's connected services

Odin by Brandefense
Research window: 1 January to 26 November 2026 (UTC; recent highlight 12 to 26 November)
Version 1.0 · Public Research Edition · TLP:CLEAR · 27 November 2026

66 of 250
assessed Czech domains showed a current credential listing on 27 November 2026

11
public-event dossiers covering confirmed Czech disruptions and disclosures

50
Czechia-labelled ransomware listings across 20 claimant labels

CZK 11.8B
attempted Czech banking fraud across 75,637 attacks in Q1 to Q3 2026

CONTENTS

Contents

01	Executive brief and defender priorities	05
	Report map	09
02	National digital profile and 2026 landscape	10
03	National exposure and selected-domain observations	17
04	Underground claims and cases	28
05	Public incidents, suppliers and recent activity	38
06	Disruption, hacktivism and claim versus reality	46
07	Ransomware, espionage advisories and threat profiles	50
08	Fraud, identity abuse and secondary harm	62
09	Banking, strong authentication and payment continuity	68
10	Regulation, reporting duties and governance	73
11	Outlook and conditional triggers for 2027	77
12	Defender action plan and remediation reference	80
A	Appendix A. Method, scope and exclusions	87
B	Appendix B. Evidence register	89
C	Appendix C. Sources	90
D	Appendix D. Glossary	95
	About this report	97

Executive / Board / CISO	01 02 05 11 12
SOC / Threat intelligence	03 04 06 07 12.2
Municipal / Public-sector IT	03 05 06 10 12
Retail / Banking / Fraud ops	04 08 09 10 12
Legal / Compliance / DPO	05 08 10 A

About this edition

Prepared with AI assistance. Evidence and limits accompany the findings.

48/100

National Atlas headline across 250 assessed Czech domains (27 November 2026 snapshot)

53,404

Czechia-tagged underground posts (1 January to 26 November 2026; 64.7% in Aug-Oct)

50

Czechia-labelled ransomware listings (1 January to 26 November 2026; 27 in full-year 2025)

CZK 11.8B

Attempted Czech banking fraud in Q1-Q3 2026 (75,637 attacks; CZK 2.2B lost)

Contents and reading routes

Chapter	Question
1 Executive brief	Which findings and decisions require leadership action first?
2 National profile	How do digital reliance, official trends and mule-chat surges shape the picture?
3 National exposure	Which credential, device and mail-policy observations require owner validation?
4 Underground claims	What do advertisements, buyer requests and recycled datasets establish?
5 Public incidents	Which publicly reported events and supplier disclosures affected Czechia?
6 Disruption and hacktivism	How do claims compare against official records and service impact?
7 Ransomware and actors	What do ransomware listings and espionage advisories establish?
8 Fraud and identity	How do leaked personal details and underground services fuel fraud?
9 Banking and strong ID	How do attackers target Bank iD, retail clients and cash-out accounts?
10 Regulation	Which authority, portal, trigger and legal deadline apply in Czechia?
11 Outlook	Which conditional triggers should shift defensive posture?
12 Action plan	Who acts, on what timeline and with what completion evidence?
Appendices A–D	Scope, evidence register, sources and definitions

CHAPTER 01

Executive brief and defender priorities

01

THIS CHAPTER ANSWERS

Which 2026 signals require action from Czech defenders today?

5

core findings grounded in distinct evidence populations

1.1 Five findings for leadership 06

1.2 Four immediate executive decisions 07

1.3 Scope and boundaries of this report 07

CHAPTER 01

Executive brief and defender priorities

IN SHORT

Czechia entered 2026 under its new Cybersecurity Act (Act No. 264/2025 Coll.) while confronting municipal ransomware, critical PHP and WordPress exploitation, third-party data breaches and CZK 11.8 billion in attempted banking fraud. Meanwhile, underground Czechia-tagged volume spiked in August to October on Russian- and Ukrainian-language Telegram bank-mule chats rather than bank breaches. Patch exposed PHP, WordPress, Citrix and router surfaces today, verify offline backups and separate client-fraud controls from perimeter defence.

1.1 Five findings for leadership

1. **Web-stack and edge flaws hit Czech institutions rapidly across 2026.** A critical WordPress flaw chain (`CVE-2026-63030` , CVSS 9.8, with `CVE-2026-60137`) drove eight revised significant Czech incidents in August [S8] [S15][S63][S77][S78]. Critical PHP flaws (`CVE-2026-109618` , `CVE-2026-109619`) hit in October [S17][S74][S75]. They triggered a two-hour precautionary website shutdown at the Office of the Government (Úřad vlády ČR), service restrictions at the Czech Hydrometeorological Institute (ČHMÚ) and active-attack containment at Czech Technical University (ČVUT) [S48][S49][S50]. Earlier, the National Cyber and Information Security Agency (NÚKIB) flagged over 3,200 Czech devices in the REDHEBERG VNC botnet [S6]. NÚKIB also documented active Czech Military Intelligence intervention against APT28 TP-Link router exploitation (`CVE-2023-50224`) [S7][S61][S84].

2. **Ransomware disrupted Czech municipalities and commercial branches while offline backups aided recovery.** Confirmed attacks hit municipal offices in Jemnice, Židlochovice, Náměšť nad Oslavou and Šumperk [S37][S38] [S39][S40][S41]. A cyberattack also exposed client data at non-bank Partners Group subsidiaries, later listed by an extortion label, and late-November ransomware hit 173 PRO-DOMA branches [S42][S43][S57]. Ransompedia logged **50 Czechia-labelled listings** across 20 claimant labels (up from **27** in full-year 2025) [S2]. Five listings, covering four confirmed public Czech cases (Partners Financial Services listed twice), match public reporting, while **45 remain unverified** [S2]. Offline backups at Náměšť nad Oslavou and PRO-DOMA's tapes enabled recovery without ransom payment [S40][S57].

3. **Third-party suppliers, support tools and legacy archives drove high-impact consumer and student exposures.** BitFaktura suffered roughly 38 hours of unauthorised database access affecting all accounts across Poland and Czechia [S44][S45]. Rohlík.cz disclosed exposure of customer-support chats, transcripts and emails from April to October [S46][S47]. Inside the 12 to 26 November window, Univerzita Karlova (Charles University) disclosed a web-application breach of central Student Information System (SIS) data [S52][S53]. That breach prompted roughly 55,000 precautionary CAS password resets [S54]. Separately, Dedoles disclosed theft of a 2021–2026 legacy e-shop backup via Slovak IT supplier `ui42` [S55][S56].

4. **Banking fraud reached CZK 11.8 billion attempted while Telegram mule-account chatter surged.** In Q1 to Q3 2026, Czech banks stopped **CZK 9.6 billion (81%)** of attempted digital fraud across **75,637 attacks** [S29][S30]. Clients still lost **CZK 2.2 billion** [S29][S30]. Police recorded **21,137 cybercrimes** in 2025 (+14.3% year on year) and a monthly record of **2,533 cases** in March 2026 [S25][S26]. In parallel, Czechia-tagged underground volume jumped

from 2,470 posts in July to **18,965 in October** (`53,404` total) [S1]. Russian- and Ukrainian-language Telegram chats drove that spike by trading bank-drop accounts (legalizační účty) and seeking Czech Bank iD and MojeID access [S1][S25][S31].

5. Portfolio exposure shows 66 domains with a current credential listing and uneven municipal hygiene. Across all 250 assessed Czech domains on 27 November 2026, the national Atlas headline stands at **48/100** [S4]. Sixty-six domains showed a current credential listing, led by retail (20), education (11) and finance (10) [S4]. On mail hygiene, **179 of 250 (71.6%)** publish DMARC `quarantine` or `reject`, and **173 (69.2%)** publish DNSSEC DS records, including all 25 central public-administration domains [S3]. Banking leads at **23 of 25** enforcing DMARC, while regional and local administration trails sharply at **11 of 25** enforced and **6 missing valid DMARC** [S3].

1.2 Four immediate executive decisions

1. **Patch exposed web stacks and edge appliances immediately.** Apply the November PHP releases (`8.5.13`, `8.4.28`, `8.3.37`, `8.2.36` or later) and fixed WordPress builds (`6.8.6+`, `6.9.5+`, `7.0.2+`) listed in §12.2 [S63][S64][S65][S74][S75][S76][S77][S78]. Also apply current Citrix NetScaler (`CTX697305`) and Zimbra releases, and retire End-of-Life routers [S62][S79][S80][S81][S83][S84].
2. **Test offline backup restoration and paper-fallback operations.** Follow the operational lessons of Náměšť nad Oslavou, Židlochovice and PRO-DOMA by verifying immutable or tape backups offline and rehearsing branch continuity without live IT [S39][S40][S57].
3. **Audit third-party access, support-tool retention and decommissioned backups.** Map every external IT supplier, revoke dormant vendor accounts and strip personal data from retired e-commerce backups [S44][S46][S55]. Restrict web-application access to central databases [S52].
4. **Verify Act No. 264/2025 Coll. registration and dual reporting channels.** Confirm whether each entity reports to NÚKIB (`GovCERT.CZ`), to `CSIRT.CZ`, or under DORA to the Czech National Bank (ČNB) [S21][S24][S27][S28]. Close monitoring-only DMARC gaps [S3].

1.3 Scope and boundaries of this report

Every figure in this report stays tied to its own population, date window and evidence level. The main activity window spans **1 January to 26 November 2026** (UTC, by publication timestamp) across underground posts (`53,404`), Ransompedia listings (`50`), 2026 domain mentions (`1,334`) and public events [S1][S2][S4]. Within that window, **12 to 26 November 2026** (`1,771` posts, `53` forum posts, and three major public disclosures) is separated in §5.3 so recent developments are never confused with full-year rates [S1][S52][S55][S57].

Brandefense Atlas exposure assessments and passive configuration checks (**all 250 domains**) reflect a **27 November 2026** snapshot, while rolling 365-day dark-chat and dark-web domain mentions span **27 November 2025 to 26 November 2026** [S3][S4]. All external advisories, Czech statutes, EU regulations and press reports were verified on **27 November 2026**. Unverified claims and criminal listings are labelled explicitly, and organisations are named only where officially confirmed and widely reported in public Czech or international media.

KEY TAKEAWAYS

01

Exposed PHP, WordPress and edge software alongside municipal and retail ransomware defined Czechia's 2026 operational risk.

02

The August-October underground spike reflects Telegram bank-drop brokerage rather than bank infrastructure compromises.

03

Patch §12.2 flaws, verify offline backups, audit suppliers and confirm Act 264/2025 or DORA reporting routes now.

Report map

Twelve chapters, five reader paths. Follow the decision that matches your responsibility; keep the evidence boundary with the finding.

Executive / Board / CISO	Which incidents, financial losses and conditional triggers shape 2027 budget and resilience?	01 02 05 11 12
SOC / Threat intelligence	Which underground listings are recycled claims, which CVEs need patching and how do claims compare to reality?	03 04 06 07 12.2
Municipal / Public-sector IT	How do local offices close the DMARC and offline-backup gap while meeting Act 264/2025 duties?	03 05 06 10 12
Retail / Banking / Fraud ops	How do Bank iD impersonation, smishing, mule accounts and supplier leaks turn into customer losses?	04 08 09 10 12
Legal / Compliance / DPO	Which deadlines apply across NÚKIB, CSIRT.CZ, ČNB (DORA), ÚOOÚ and EU CRA Article 14?	05 08 10 A

CHAPTER 02

National digital profile and 2026 landscape

02

THIS CHAPTER ANSWERS

How do Czechia's digital reliance and institutional shift shape its 2026 threat surface?

94.2%

internet penetration across 9.96 million users

2.1 Digital connectivity, shared identity rails and civic context 11

2.2 Official Czech threat tempo from 2025 into late 2026 11

2.3 Interpreting Czechia's underground publication volume 13

CHAPTER 02

National digital profile and 2026 landscape

IN SHORT

Czechia combines near-universal internet use, rapid Bank iD adoption and an export-oriented industrial base with new cybersecurity duties under Act No. 264/2025 Coll. Official NÚKIB tracking logged 215 revised incidents across January to October 2026 while police cybercrime reached record monthly levels. Meanwhile, Czechia-tagged underground volume jumped in August to October on Russian- and Ukrainian-language Telegram bank-mule chats. Filter out multi-country mule templates so alerts focus on genuine Czech web-stack, ransomware and fraud signals.

2.1 Digital connectivity, shared identity rails and civic context

At the start of 2026, Czechia's population of **10.6 million** included **9.96 million internet users (94.2% penetration)** [S66]. Mobile adoption reached **14.7 million cellular connections (139% of population)**, alongside **8.08 million social-media user identities (76.4%)** [S66]. Everyday citizen and business workflows rely heavily on digital public services such as Portál občana (Citizen Portal), Datové schránky (statutory electronic data boxes), `MojeID` and bank-issued electronic identity (`Bank iD`) [S31][S32]. High digital concentration delivers speed for taxpayers, shoppers and firms, yet also makes shared identity portals and commercial e-commerce platforms attractive impersonation lures [S31][S32].

Czechia's 2026 institutional calendar added routine public-sector transition alongside steady operational demand. Following the October 2025 parliamentary election, a new government took office and faced a confidence vote in early 2026, while municipal and Senate elections took place in October 2026 [S67]. On 7 January 2026, the State Security Council published an official statement on Czechia's continued role in the international ammunition initiative for Ukraine [S36]. Two days later, hacktivist channels referenced ammunition deliveries when threatening Czech government websites, alongside the January DDoS wave reported by NÚKIB [S1][S9][S36].

2.2 Official Czech threat tempo from 2025 into late 2026

Official reporting from NÚKIB, CSIRT.CZ, the Ministry of the Interior (MV ČR) and the Office for Personal Data Protection (ÚOOÚ) shows elevated operational pressure before and throughout 2026. In its 2025 Annual Report, NÚKIB recorded **203 cyber incidents** in 2025 (down from 268 in 2024), comprising **2 very important**, **12 important** and **189 less important** events [S5].

That 2025 review documented four baseline milestones prior to our 2026 window. First, Czechia publicly attributed a 2022–2024 intrusion into the Ministry of Foreign Affairs unclassified network to **APT31** in May 2025 (cited strictly as pre-2026 context) [S5]. Second, Europol-led **Operation Eastwood** disrupted `NoName057(16)` infrastructure in July 2025 [S5][S85]. Third, NÚKIB issued two 2025 warnings concerning DeepSeek and data transfers to the People's Republic of China [S5]. Fourth, the government approved the **National Cyber Security Strategy 2026–2030** in September 2025 [S20].

Across **January to October 2026**, NÚKIB's revised quarterly and October monthly totals reached **215 recorded incidents** (`Q1: 75` , `Q2: 44` , `Q3: 65` , `October: 31`) [S6][S7][S8][S17]. Summing initial monthly releases yields **218** because NÚKIB retroactively reclassifies incidents in quarterly reviews [S7][S8]. Specifically, April moved from 18 initial to 16 revised, August moved from 28 initial to 27 revised, and one Q1 incident was later upgraded to very important [S7][S8][S12][S15].

Monthly figures ran as follows across the ten reported months. Q1 logged January **32** (1 significant), February **23** (2 significant) and March **20** (4 significant) [S6][S9][S10][S11]. Q2 logged April **16** revised (18 initial), May **12** and June **16** [S7][S12][S13]. Q3 and October logged July **12**, August **27** revised (28 initial; 8 significant), September **26** (1 significant) and October **31** (5 significant; 4 DDoS) [S8][S14][S15][S16][S17].

Period (2026)	NÚKIB revised total	Significant / very significant	Dominant operational drivers reported by NÚKIB	Sources
Q1 (Jan–Mar)	75	6 significant, 1 very significant (reclassified in Q2 review)	Early-year DDoS waves (`NoName057(16)` , `ServerKillers`), REDHEBERG VNC botnet (>3,200 Czech devices), APT28 `Operation Neusploit` (`CVE-2026-21509`)	[S6][S7][S9][S10][S11]
Q2 (Apr–Jun)	44	6 significant, 0 very significant	APT28 TP-Link router exploitation (`CVE-2023-50224`) with Military Intelligence active intervention, FortiBleed exposure, Czech Police smishing, SparkyCarp phishing against Evropské hodnoty	[S7][S12][S13]
Q3 (Jul–Sep)	65	13 significant (4 Jul, 8 Aug, 1 Sep), 0 very significant	WordPress `wp2shell` intrusion surge (~two-thirds of Q3 in NÚKIB's Intrusion category), STORM-2372, LAUNDRY BEAR Zimbra (`CVE-2025-66376`), BlueMoon exploit kit, Tenda/Zbtlink backdoors	[S8][S14][S15][S16]

Period (2026)	NÚKIB revised total	Significant / very significant	Dominant operational drivers reported by NÚKIB	Sources
October	31	5 significant, 0 very significant	PHP2Shell (`CVE-2026-109618` , `CVE-2026-109619`) wave hitting public bodies and universities, ~half Intrusion, 4 DDoS incidents	[S17][S48][S49]
Jan–Oct total	**215**	**30 significant, 1 very significant**	**Measured during Act 264/2025 one-year reporting ramp (initial monthly sum: 218)**	[S6][S7][S8][S17]

NÚKIB explicitly cautions against reading early-2026 dips or rises as raw national prevalence changes [S7][S8]. Act No. 264/2025 Coll. took effect on **1 November 2025**, initiating a staged registration and one-year compliance ramp (`Section 15(4)`) while shifting lower-obligation reporting from NÚKIB to `CSIRT.CZ` [S7][S8][S21][S24]. Outside NÚKIB's regulated perimeter, **CSIRT.CZ** handled **3,005 incidents in 2025** (up over 30% year on year, led by phishing) [S23]. On **24 November 2026**, CZ.NIC and NÚKIB signed a renewed public-law contract confirming CZ.NIC's National CSIRT mandate for lower-obligation entities [S24].

Law-enforcement and privacy totals point in the same upward direction. In 2025, Czech police registered **21,137 cybercrimes** (+2,642 cases or **+14.3%** year on year) [S25]. Cybercrime reached **12.4%** of all recorded crime even as overall crime fell 1.9% [S25]. Clearance stood at **15.1%**, with **1,224** cases recorded under qualified computer-crime offences (`Sections 230–232` of the Criminal Code) [S25].

In **March 2026**, police recorded a monthly high of **2,533 cybercrime cases** (+37% year on year), driven heavily by fake-banker and fake-police voice scams totaling **CZK 322 million** in early-year losses [S26]. Separately, ÚOOÚ recorded a historic high of **392 personal-data breach notifications** in 2025 (up from 336 in 2024) alongside **3,854 citizen submissions** (+68%) and **1,430 spam complaints** [S33].

2.3 Interpreting Czechia's underground publication volume

Between **1 January and 26 November 2026**, Brandefense observed **53,404 Czechia-tagged underground posts** [S1]. Monthly volume stayed steady between **1,689 and 2,470 posts per month** from January through July [S1]. Volume then jumped sharply in **August (6,655)**, **September (8,940)** and **October (18,965)** before easing to **3,893** across the partial 1 to 26 November window [S1]. Together, August through October account for **34,560 posts (64.7%)** of the entire eleven-month Czechia-tagged total [S1].

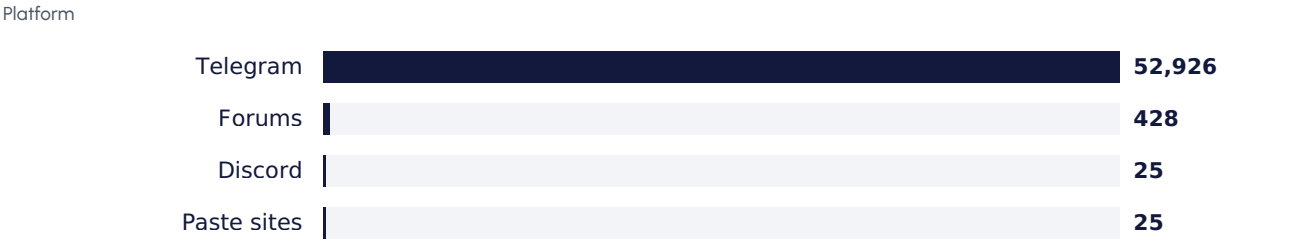
August to October Telegram bank-drop chatter drove 64.7% of Czechia-tagged underground volume



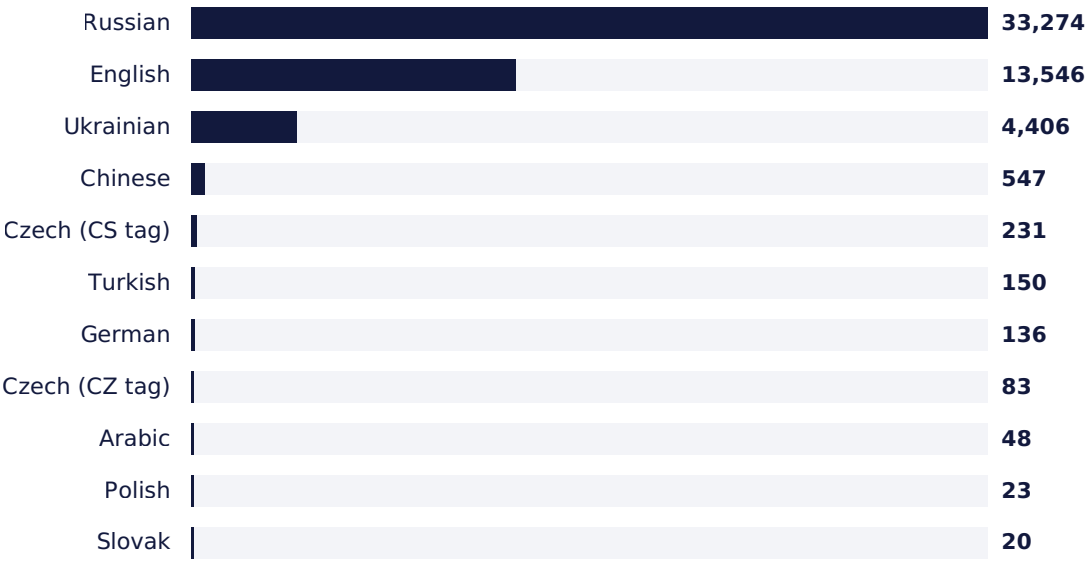
Source: Odin by Brandefense, 53,404 Czechia-tagged underground posts, 1 January-26 November 2026; November partial [S1]. Posts are not confirmed incidents; language tags can overlap.

Inspecting platform, language and content categories explains that surge cleanly and prevents misreading it as a wave of Czech corporate breaches. Across the full window, **Telegram** accounts for **52,926 posts (99.1%)**, followed by **forums (428; 0.8%)**, **Discord (25)** and **paste sites (25)**, with **zero Tor** entries [S1]. By language tag (where multi-language posts may carry more than one tag), **Russian (** `33,274` **)**, **English (** `13,546` **)** and **Ukrainian (** `4,406` **)** dominate [S1]. Smaller shares carry **Chinese (** `547` **)**, **Czech (** `CS 231` **and** `CZ 83` **)**, **Turkish (** `150` **)**, **German (** `136` **)**, **Arabic (** `48` **)**, **Polish (** `23` **)** and **Slovak (** `20` **)** tags [S1].

Telegram accounts for 99.1% of Czechia-tagged posts, led by Russian, English and Ukrainian



Language



Source: Odin by Brandefense, 53,404 Czechia-tagged underground posts, 1 January–26 November 2026; November partial [S1]. Posts are not confirmed incidents; language tags can overlap.

Content review shows that the August–October spike is overwhelmingly **bank-drop and KYC brokerage** rather than enterprise intrusion trading [S1]. Posts on financial-account buying and renting climbed from **458 in July** to **2,770 in August**, **6,240 in September** and **13,457 in October** (71.0% of October's total) [S1]. That rise matched Russian (`14,083`) and Ukrainian (`2,697`) language peaks in October [S1]. The full eleven-month period shows **28,287 financial-account sale or rental posts** and **19,599 KYC-document posts**, compared with **4,185 data-leak/database posts** and **2,775 access-sale posts** [S1].

On forums, November's rise to **101 Czechia-tagged forum posts** (of **428**) includes many generic international threads that do not target Czech organisations [S1]. The genuine Czech forum listings are examined in Chapter 4 and §5.3 [S1].

Czechia avoided Germany's early-year bulk wave but recorded a distinct August to October Telegram mule surge



August-October 2026 surge window only (separate scale)



Country-tagged raw posts across monitored channels; not adjusted for population or source coverage. Source: Odin by Brandefense, 53,404 Czechia-tagged underground posts, 1 January-26 November 2026; November partial [S1]. Posts are not confirmed incidents; language tags can overlap.

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

Comparing Czechia against its four immediate regional neighbours (`Slovakia`, `Poland`, `Austria` and `Germany`) clarifies both scale and wave structure [S1]. Over 1 January to 26 November 2026, total country-tagged posts and forum counts were **Czechia 53,404 (428 forum)**, **Slovakia 20,041 (127 forum)** and **Austria 34,482 (320 forum)** [S1]. Larger neighbours logged **Poland 118,972 (726 forum)** and **Germany 1,223,609 (2,606 forum)** [S1]. Germany absorbed an enormous January–February bulk spam wave (`429,473` in January and `417,736` in February) that bypassed Czechia [S1]. By contrast, Czechia experienced a concentrated autumn surge in Russian- and Ukrainian-language Telegram bank-drop chats aligned with Central European cash-out rails [S1].

KEY TAKEAWAYS

01

NÚKIB logged 215 revised incidents across January to October 2026 while police cybercrime and ÚOOÚ breach notices hit record highs.

02

August-October's surge to 18,965 monthly posts reflects Telegram bank-mule and KYC brokerage, not Czech bank compromises.

03

Separate Telegram drop-broker chatter and generic international threads from verified forum listings in security triage.

CHAPTER 03

National exposure and selected-domain observations

03

THIS CHAPTER ANSWERS

Which exposure signals and configuration gaps require validation across 250 Czech domains?

66 of 250

assessed Czech domains showed a current credential listing on 27 November 2026

3.1 Universe card and assessment boundary 18
3.2 National Atlas headline and current credential listings 19
3.3 Infected-device and historical credential-record associations 21
3.4 Documents, similar domain names and 365-day underground mentions 24
3.5 Mail authentication, DNSSEC, TLS and HSTS across 250 Czech domains 24
3.6 Turning exposure signals into separate validation queues 27

CHAPTER 03

National exposure and selected-domain observations

IN SHORT

Across all 250 assessed Czech domains on 27 November 2026, the national Atlas headline is 48/100. Sixty-six domains showed a current credential listing, 221 had at least 318,706 device associations and 231 had 180,747,551 historical credential records (99.4% concentrated in telecom and consumer webmail). Nationally, 71.6% enforce DMARC and 69.2% sign DNSSEC, yet regional and local administration lags at 11 of 25 enforcing DMARC. Triage current listings within five days, reconcile employee devices separately from customers and close monitoring-only DMARC gaps.

3.1 Universe card and assessment boundary

To establish a reproducible national baseline without naming private portfolio members, Brandefense assembled a purposive portfolio of **250 Czech domains** divided into **ten equal sector cells of 25 domains each** [S3]. All **250** were assessed on **27 November 2026** [S3][S4]. The ten cells span central ministries and agencies, regional and municipal offices, licensed banks and insurers, energy utilities, telecom and digital platforms, major manufacturers, transport operators, hospitals, universities and large retailers [S3].

Portfolio parameter	Value	Operational meaning and boundary	Sources
Selected and assessed domains	250 of 250 (10 cells × 25)	Purposive national sample; not a statistical census of all Czech entities	[S3][S4]
National Atlas headline	**48/100** (27 November 2026)	Single portfolio-wide exposure headline; no per-sector, group or organisation ratings published	[S4]
Exposure snapshot signals	27 November 2026 (250/250 assessed)	Cumulative signals that may overlap; never represent unique people, 2026-only activity or confirmed incidents	[S4]
Passive configuration snapshot	27 November 2026 (250/250 assessed)	Published DNS, mail-policy, TLS and HTTP header states on that date	[S3]
Rolling 365-day domain mentions	27 November 2025 to 26 November 2026	Domain mentions on dark chat and dark web; 2026 subset (1 Jan to 26 Nov) kept separate	[S4]

Three strict interpretation rules govern Chapter 3. First, only the single national Atlas headline (**48/100**) is published across the full 250-domain portfolio; no sector or organisation ratings appear anywhere in this report [S4]. Second, exposure counts (device associations, historical credentials, documents and similar-name observations) are cumulative external observations that may overlap across domains and individuals and do **not** establish a server breach [S4]. Third, published DNS records (`DMARC` , `SPF` , `DKIM` , `DNSSEC` , `CAA`) and published TLS/HSTS states describe external configuration rather than internal network resilience [S3][S70][S71][S72][S73]. Endpoints that were unreachable on the snapshot date are reported as a separate count [S3].

3.2 National Atlas headline and current credential listings

On the **27 November 2026** snapshot, the single national Atlas headline across all **250 assessed Czech domains** stands at **48/100** [S4]. Across the portfolio, **66 of 250 domains (26.4%)** showed a **current credential listing** (all 66 with listing history, totaling **5,431 historical entries**) [S4]. Current listings represent the highest-priority signal for immedi-
ate owner verification because they indicate active marketplace offers referencing a domain's credentials [S4].

Current credential listings and exposure signals across 250 assessed Czech domains

	Current listings	With devices	Employee devices	With credentials	With documents	Similar names (30d)
Public administration	1/25	13/25	7/25	15/25	7/25	23/25
Regional and local administration	1/25	22/25	11/25	22/25	10/25	21/25
Banking and finance	10/25	22/25	16/25	24/25	12/25	22/25
Energy and utilities	4/25	21/25	16/25	25/25	4/25	18/25
Telecom and digital services	7/25	25/25	22/25	25/25	15/25	21/25
Industry and manufacturing	0/25	22/25	17/25	22/25	5/25	17/25
Transport, logistics and postal	9/25	22/25	14/25	24/25	7/25	22/25
Health and life sciences	3/25	24/25	19/25	24/25	6/25	13/25
Education and research	11/25	25/25	24/25	25/25	20/25	22/25
Retail, media and consumer services	20/25	25/25	22/25	25/25	15/25	22/25

Current credential listings by sector (coral). Each cell shows observed domains / 25 assessed domains; signals overlap. Source: Brandefense exposure observations for all 250 assessed Czech domains, 27 November 2026 snapshot [S4]. Cumulative associations can overlap; they are not unique people or confirmed intrusions.

Sector-level counts below show how widely each exposure signal appears across the ten equal 25-domain cells [S4]:

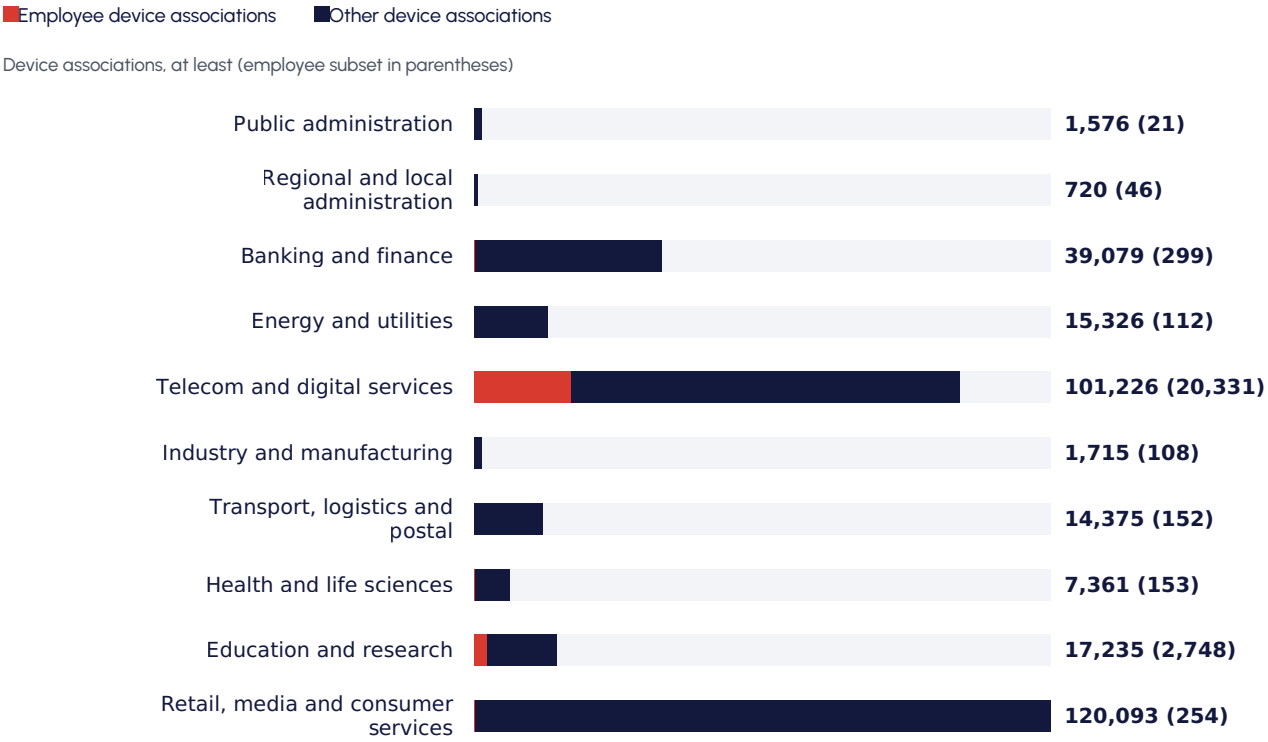
Sector cell (25 domains each)	Assessed	Domains with devices	Domains with employee devices	Domains with credentials	Current credential listings	Sale history	30d similar names	Exposed docs
Public administration	25	13	7	15	1	1	23	7
Regional and local administration	25	22	11	22	1	1	21	10
Banking and finance	25	22	16	24	10	10	22	12
Energy and utilities	25	21	16	25	4	4	18	4
Telecom and digital services	25	25	22	25	7	7	21	15
Industry and manufacturing	25	22	17	22	0	0	17	5
Transport, logistics and postal	25	22	14	24	9	9	22	7
Health and life sciences	25	24	19	24	3	3	13	6
Education and research	25	25	24	25	11	11	22	20
Retail, media and consumer services	25	25	22	25	20	20	22	15
Total	**250**	**221**	**168**	**231**	**66**	**66**	**201**	**101**

Current credential listings cluster heavily in high-volume consumer, academic and financial environments [S4]. **Retail, media and consumer services** leads with **20 of 25 domains**, followed by **Education and research (11)**, **Banking and finance (10)**, **Transport, logistics and postal (9)** and **Telecom and digital services (7)** [S4]. By contrast, **Industry and manufacturing** logged **zero current listings**, and both **Public administration** and **Regional and local administration** logged **1 domain each** [S4]. Portfolio listings are not linked to any named organisation in this report.

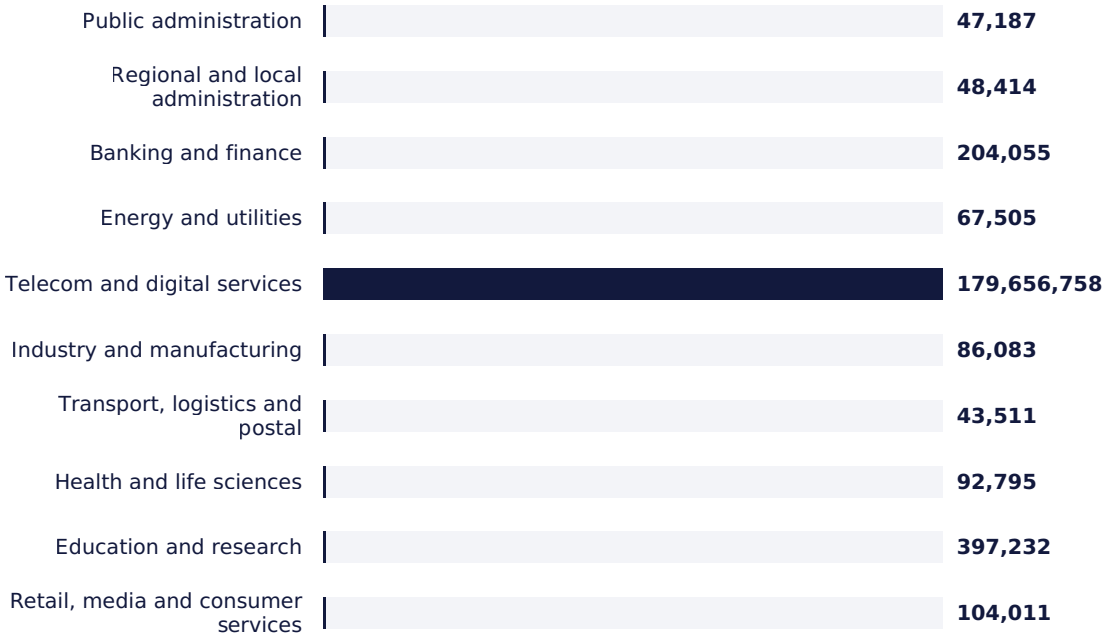
3.3 Infected-device and historical credential-record associations

Across all **250 assessed Czech domains**, **221 domains (88.4%)** showed **at least 318,706 device associations**, splitting into **24,224 employee-labelled device associations** (across **168 domains**) and **294,482 non-employee device associations** [S4]. Separately, **231 domains (92.4%)** accumulated **180,747,551 historical credential record associations**: **86,659,575** from breach databases, **9,161,620** from infostealers and **84,926,356** from combolists [S4].

Device and credential-record associations concentrate in telecom, retail, banking and education



Credential-record associations (separate scale; Telecom holds 99.4%)



Source: Brandefense exposure observations for all 250 assessed Czech domains, 27 November 2026 snapshot [S4]. Cumulative associations can overlap; they are not unique people or confirmed intrusions.

Sector cell (25 assessed each)	Device associations (at least)	Employee devices	Non-employee devices	Credential records total	Breach DB records	Stealer records	Combolist records	Exposed docs	30d similar names
Public administration	1,576	21	1,555	47,187	12,229	1,049	33,909	11	3,614
Regional and local administration	720	46	674	48,414	26,177	2,115	20,122	16	22,073
Banking and finance	39,079	299	38,780	204,055	130,196	6,224	67,635	34	3,821
Energy and utilities	15,326	112	15,214	67,505	39,192	1,755	26,558	6	6,178
Telecom and digital services	101,226	20,331	80,895	179,656,758	86,204,733	9,056,551	84,395,474	765	12,504
Industry and manufacturing	1,715	108	1,607	86,083	53,588	3,091	29,404	11	4,679

Sector cell (25 assessed each)	Device associations (at least)	Employee devices	Non-employee devices	Credential records total	Breach DB records	Stealer records	Combolist records	Exposed docs	30d similar names
Transport, logistics and postal	14,375	152	14,223	43,511	16,173	3,918	23,420	10	11,751
Health and life sciences	7,361	153	7,208	92,795	49,064	4,193	39,538	10	98
Education and research	17,235	2,748	14,487	397,232	85,145	73,664	238,423	94	721
Retail, media and consumer services	120,093	254	119,839	104,011	43,078	9,060	51,873	53	2,806
Total (250 assessed)	**318,706**	**24,224**	**294,482**	**180,747,551**	**86,659,575**	**9,161,620**	**84,926,356**	**1,010**	**68,245**

Three structural patterns explain these totals and guide defender triage [S4]:

- **Consumer webmail concentration explains 99.4% of historical credentials.** Telecom and digital services accounts for **179,656,758** of the **180,747,551** credential records (**99.4%**) [S4]. Dominant Czech consumer webmail portals accumulate decades of reused third-party breach and combolist logins without implying operator server compromise [S4]. Excluding Telecom and digital services, the other nine sectors combined hold **1,090,793** historical credential records, led by **Education and research (397,232)**, **Banking and finance (204,055)** and **Retail (104,011)** [S4].
- **Customer devices dominate Retail and Banking while Education carries heavy staff exposure.** Retail holds **120,093** device associations (**119,839** non-employee vs **254** employee), and Banking holds **39,079** (**38,780** non-employee vs **299** employee) [S4]. By contrast, **Education and research** records **2,748 employee-labelled devices** across **24 of 25** domains, reflecting large mixed managed and unmanaged university fleets [S4]. On consumer webmail domains inside Telecom (`20,331` employee-labelled devices), many associations may belong to private users rather than staff, so reconcile against internal endpoint inventories before acting [S4].
- **Cumulative records are not 2026-only breach counts.** Historical credential and device counts aggregate multi-year records across overlapping individuals and domains [S4]. Defenders must never treat cumulative exposure totals as 2026 compromise counts [S4].

3.4 Documents, similar domain names and 365-day underground mentions

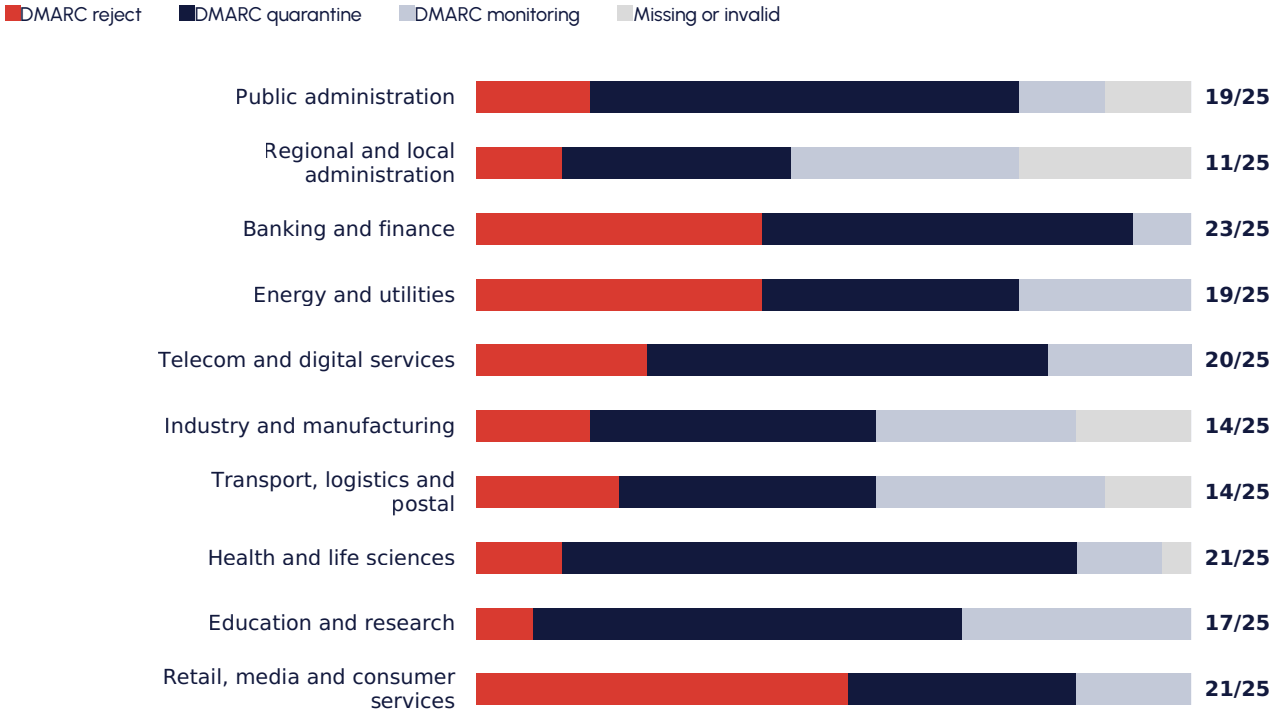
Beyond credentials and devices, **101 of 250 domains** showed **1,010 exposed document associations** (led by Telecom with **765**, Education **94**, Retail **53** and Banking **34**) [S4]. Separately, **201 domains** showed **68,245 30-day similar-name observations** [S4]. High totals appear in **Regional and local administration (22,073)**, **Telecom (12,504)** and **Transport (11,751)** [S4]. Short municipal or generic brand strings often resemble unrelated global domains, so lookalike alerts require phishing-intent validation before takedown [S4].

Over the separate rolling 365-day window (**27 November 2025 to 26 November 2026**), **33 of 250 selected Czech domains (13.2%)** recorded **1,931 dark-chat mentions**, while **16 domains (6.4%)** recorded **230 dark-web mentions** [S4]. Inside the strict 2026 window (**1 January to 26 November 2026**), **23 domains (9.2%)** generated **1,334 domain mentions** [S4]. Telecom and digital services concentrated **1,785 of 1,931 dark-chat mentions (92.4%)**, **193 of 230 dark-web mentions (83.9%)** and **1,291 of 1,334 mentions in 2026 (96.8%)** on consumer webmail and digital-service domains [S4]. Retail followed with **108 dark-chat mentions**, whereas **Energy and utilities** logged zero and **Banking and finance** logged only **2 domains (3 dark-chat mentions, 0 dark-web)** [S4].

3.5 Mail authentication, DNSSEC, TLS and HSTS across 250 Czech domains

Passive inspection on **27 November 2026** reveals a comparatively mature Czech baseline for DNS cryptographic signing and sender authentication, paired with sharp sectoral disparities in municipal and industrial DMARC enforcement [S3]. Across all 250 domains, **179 (71.6%)** publish DMARC policies requesting `quarantine` (**119**) or `reject` (**60**), **54 (21.6%)** remain in monitoring mode (`p=none`), and **17 (6.8%)** lack a valid DMARC record [S3][S70].

Banking and retail lead DMARC enforcement while regional and local administration trails sharply



Right-hand values show enforced (reject or quarantine) / 25 selected domains per sector. Source: passive configuration observations for 250 selected Czech domains, 27 November 2026 snapshot [S3]. Published policies do not establish message-level enforcement or prevented spoofing.

Supporting mail, DNS and transport controls show equally informative national strengths and gaps across the 250-domain snapshot [S3]:

Sector cell (25 domains each)	DMARC reject	DMARC quarantine	DMARC none	DMARC missing/ invalid	DNSSEC DS	SPF present	DKIM found	CAA present	HSTS set
Public administration	4	15	3	3	25	24	18	17	22
Regional and local administration	3	8	8	6	18	23	14	3	16
Banking and finance	10	13	2	0	20	25	20	9	21
Energy and utilities	10	9	6	0	20	25	20	4	16

Sector cell (25 domains each)	DMARC reject	DMARC quarantine	DMARC none	DMARC missing/ invalid	DNSSEC DS	SPF present	DKIM found	CAA present	HSTS set
Telecom and digital services	6	14	5	0	16	23	21	8	20
Industry and manufacturing	4	10	7	4	11	24	18	2	15
Transport, logistics and postal	5	9	8	3	13	25	18	3	15
Health and life sciences	3	18	3	1	19	25	20	7	10
Education and research	2	15	8	0	18	25	20	11	17
Retail, media and consumer services	13	8	4	0	13	25	22	4	11
Total (250 domains)	**60**	**119**	**54**	**17**	**173**	**244**	**191**	**68**	**163**

Five technical findings warrant direct defender follow-up [S3]:

- **Exceptional DNSSEC adoption led by central government.** Czechia's `.cz` registry culture shows clearly: **173 of 250 domains (69.2%)** publish DNSSEC DS records [S3]. Adoption hits **25 of 25 (100%)** in Public administration and **20 of 25 (80%)** in both Banking and Energy [S3]. Industry and manufacturing (**11/25**) and Transport (**13/25**) sit farthest behind [S3].
- **Regional and local administration is the single widest DMARC gap.** Only **11 of 25 (44%)** regional and municipal domains enforce DMARC (`3 reject`, `8 quarantine`) [S3]. Eight stay in `none` and **6** lack any valid DMARC policy [S3]. Combined with **14 of 25** enforced in Industry (4 missing) and **14 of 25** in Transport (3 missing), **71 of 250 domains (28.4%)** remain open to direct-domain spoofing [S3][S70].

- **High SPF and DKIM presence makes DMARC upgrades low-friction.** Already, **244 of 250 domains (97.6%)** publish SPF and **191 (76.4%)** had a DKIM record found [S3][S71][S72]. Most of the 54 monitoring-mode domains can therefore advance toward `quarantine` or `reject` after reviewing alignment reports [S3][S70]. Notice that published DMARC policy tags do not by themselves establish `pct=100` coverage or guarantee receiver enforcement under RFC 7489 [S70].
- **TLS, HSTS and CAA posture across reachable endpoints.** Across the 250 domains, **238** presented valid TLS certificates, **4** failed TLS validation and **8** could not be assessed on the snapshot date [S3]. Among **227** reachable HTTP endpoints (23 unavailable), **163 (71.8% of reachable)** set HSTS headers [S3][S73]. Public administration (22) and Banking (21) led HSTS adoption, while Health (10) and Retail (11) lagged [S3]. CAA certificate-authority constraints appeared on **68 of 250 domains (27.2%)** [S3].
- **Mail-hosting diversity makes on-premises patching critical.** Mail routing split across **88 domains (35.2%)** using Microsoft 365 MX records, **14** using Google Workspace and **4** with no MX record [S3]. The remaining **144 domains (57.6%)** run domestic, European or self-hosted mail servers [S3]. Patching on-premises mail software (such as Zimbra `CVE-2025-66376`) is therefore just as vital as cloud M365 defence [S3][S8][S83].

3.6 Turning exposure signals into separate validation queues

Defenders should route these findings into three distinct operational queues rather than blending them into one alert stream:

1. **Current credential-listing queue (within 5 working days).** Validate the **66 domains** with active credential listings against live identity logs, force token revocations where matched and document dated closures [S4].
2. **Split device-triage queue (30 days).** Reconcile employee-labelled device associations (`24,224` across `168` domains) against corporate endpoint inventories and keep non-employee device signals (`294,482`) routed to customer-fraud controls [S4].
3. **Messaging and DNS hardening queue (30 days).** Audit the **71 domains** lacking enforcing DMARC (prioritising municipal, manufacturing and transport domains) [S3][S70]. Fix the **4 invalid TLS certificates** and enable HSTS and CAA on public portals [S3][S73].

KEY TAKEAWAYS

01

Across all 250 assessed Czech domains on 27 November 2026, the national Atlas headline is 48/100, with 66 showing current credential listings and 221 linked to at least 318,706 device associations.

02

Telecom webmail portals hold 99.4% of the 180.7M historical credential records, while regional and local administration shows Czechia's widest DMARC gap (11 of 25 enforced, 6 missing).

03

Triage current listings within five working days, reconcile employee devices separately from customers and move the 71 non-enforcing domains to quarantine or reject.

CHAPTER 04

Underground claims and cases

04

THIS CHAPTER ANSWERS

What are threat actors actually advertising, seeking and recycling around Czechia?

7

documented underground claim cases across 16 verbatim post cards

4.1 How to read underground claims 29

4.2 Database sales, recycled dumps and inflated claims 29

4.3 Access brokers, mislabelled combos and webmail checkers 32

4.4 Telecom bypasses, forged KYC documents and Czech strong-ID demand 35

CHAPTER 04

Underground claims and cases

IN SHORT

Observed underground posts show an active market around Czech data, credentials, telecom bypasses, forged KYC documents and Bank iD or mule accounts. Yet forensic comparison shows heavy recycling and mislabelling. A 22 November "Year: 2026 Fresh" e-shop listing matches a February schema whose timestamps ended in November 2025, and a 121K "Czech Republic" combo points to `argentina.txt`. Verify every underground claim against live schemas and historical archives before triggering incident or regulatory escalations.

4.1 How to read underground claims

An underground advertisement establishes only one verified fact: a threat actor published an offer or buyer request on a given date [S1]. It does **not** establish that a Czech organisation was breached, that the data is current, or that a transaction succeeded [S1]. To protect unverified targets and avoid amplifying extortion claims, all unconfirmed company names, victim domains, exact localities and poster handles are withheld across Cases A through G and Post Cards `B01` through `B16`.

4.2 Database sales, recycled dumps and inflated claims

CASE A

A

Claimed Czech telecom export and forensic evidence of e-shop dump recycling

Claims unverified

Telecom, retail and web portals

Bottom line

Check advertised table schemas and sample timestamps against live exports and prior archives before issuing breach notices.

Evidence card B01 — 18 Feb 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

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.

Note. The named provider is withheld because no official breach confirmation was identified.

Held

A forum seller uses a recurring three-section template to advertise purported contact, booking and identity-verification tables attributed to a Czech telecommunications provider.

Not established

Authenticity, fresh capture, server intrusion, affected record count or any completed sale.

Evidence card B02 — 24 Feb 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

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

Note. All customer names, email addresses and the retailer's domain are removed; B13 re-advertises the same schema nine months later as a fresh 2026 database.

Held

A February forum post leaks a purported 105,000-line Czech online retailer customer file whose sample timestamps end in late November 2025.

Not established

Original intrusion date, complete-file integrity, active passwords or official breach confirmation.

Evidence card B13 — 22 Nov 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

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]

Note. Two additional 22 November listings on the same forum claimed datasets from an unnamed Czech web portal (three-table template) and a Czech internet provider; one listing left automated schema-inference boilerplate.

Held

On 22 November 2026, a forum seller re-advertises the same ~105,000-row Czech e-commerce schema first posted in February (B02) as a 'Fresh' 2026 database.

Not established

Any November 2026 intrusion, newly captured customer records or official breach confirmation.

Three forum threads across February and November 2026 illustrate both structured database marketing and systematic date-laundering [S1]. On **18 February**, a forum seller posted a three-section export attributed to a Czech telecom operator (`B01`), structured into customer profile, order and billing segments [S1]. On **24 February**, another thread offered a roughly **105,000-row** Czech e-commerce dataset (`B02`) whose sample schema showed order timestamps ending on **25 November 2025** [S1].

Nine months later, on **22 November 2026**, a seller re-advertised the **exact same ~105,000-row schema** labelled **"Year: 2026 Fresh"** (`B13`) [S1]. Two additional 22 November Czech database threads appeared the same day, including one that left AI-generated schema-inference boilerplate inside the description [S1]. None of the underlying targets publicly confirmed a matching 2026 breach, and all unconfirmed company names are withheld [S1]. For Czech SOC teams, Case A provides a concrete verification rule: archive sample column headers and maximum timestamps from historical listings so recycled "fresh" leaks are dismissed rapidly [S1].

CASE B

B

Unverified 6.5-million-row Czech financial contact claim on Telegram

Claim unverified

Financial and insurance data

Bottom line

Treat unattributed multi-million-row Telegram database claims as unverified until custodian logs or sample records show real internal origin.

Evidence card B03 29 Jan 2026

Channel poster (alias withheld) Telegram channel Telegram Russian

ORIGINAL

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.

TRANSLATION

A Czech database is for sale. 6.5 million rows (3 banks, one insurance company). Has not been publicly available. [...] Fields: phone number, full name, street, house, apartment, city, postal code. Sold from 100k rows at a time.

Note. No institution names or verifiable samples accompany the post; marketing phrases such as 'primary source' do not establish bank compromise.

Held
A Russian-language Telegram listing advertises a purported 6.5-million-row Czech contact dataset attributed generically to three banks and one insurer, sold in 100,000-row lots.

Not established
Any intrusion at a Czech bank or insurer, record count accuracy, unique individuals, fresh capture or completed sale.

On **29 January 2026**, a Russian-language Telegram seller advertised a claimed **6.5 million Czech consumer records** attributed to "3 banks and 1 insurer", offered for sale in **100,000-row lots** (`B03`) [S1]. No Czech bank or insurer confirmed a matching mass breach, and no verifiable unique institutional identifiers accompanied the

listing [S1]. Large round-number Telegram claims targeting Czechia frequently aggregate scraped marketing directories, older unrelated files or foreign contact tables repackaged under domestic financial labels [S1]. Defenders should require verifiable customer-specific fields that exist only in internal systems before treating million-row Telegram claims as live compromises [S1].

4.3 Access brokers, mislabelled combos and webmail checkers

CASE C

C

Initial-access broker offering claimed Czech financial-services RDP

Offer unverified

Financial services access

Bottom line

Remove direct RDP from the public internet, enforce phishing-resistant MFA on remote access and audit privileged Linux and Windows logins.

Evidence card B04 14 Apr 2026

Forum poster (alias withheld) Forum thread Forum English

ORIGINAL

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

Note. Published in April, when NÚKIB reported that intrusions accounted for half of all recorded Czech incidents.

Held

An April forum listing advertises purported remote-desktop access to an unnamed Czech financial-services host alongside an endpoint-agent label.

Not established

Active access validity, victim identity, privileged compromise, consistency of the technical labels or any completed transfer.

On **14 April 2026**, a forum initial-access broker advertised `[RDP] Financial Services - Czech Republic (B04)` [S1]. While the underlying access claim remains unverified and no Czech financial institution was named or confirmed, the listing documents steady broker demand for exposed Remote Desktop Protocol endpoints inside Central European financial firms [S1]. Financial and advisory IT teams should eliminate direct internet-facing RDP, mandate phishing-resistant MFA on all remote-access gateways and hunt for anomalous remote sign-ins matching April and subsequent access-broker postings [S1].

CASE D

D

Mislabelled foreign combos, URL-filtered stealer extracts and Czech webmail checkers

Consumer mail and portals

Claims unverified

Bottom line

Treat URL-bound credential extracts as likely end-user device theft, inspect file provenance for mislabelled dumps and block credential stuffing.

Evidence card B05 — 24 Jan 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

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

Note. File-hosting links and handles are removed; the mis-matched filename illustrates how recycled global dumps are routinely relabelled by country.

Held

A January forum post promotes a 121,000-line 'FRESH | HQ' Czech email-and-password combo whose own file-host mirror carries the filename argentina.txt.

Not established

Czech origin of the rows, working credentials, fresh 2026 compromise or single-organisation provenance.

Evidence card B06 — 15 May 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

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

Note. URL-filtered extracts ordinarily reflect end-user device credential theft rather than compromise of the named service.

Held

A May forum upload distributes 100 URL, username and password lines filtered for a Czech telecommunications customer portal (paired with a parallel 100-line Czech streaming-service extract on the same day).

Not established

Server-side intrusion at either Czech provider, current password validity or active account takeover.

Evidence card B07 — 2 Mar 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

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

Note. Download URLs are removed; recurring small-batch mail-access threads test reused passwords across Czech webmail and corporate domains.

Held

A March forum listing distributes a 17,000-line credential compilation labelled for .cz email domains, alongside recurring monthly 1,000-line Czech mail-access batches across February through October.

Not established

Current mailbox access, unique individuals, fresh capture date or institutional breach provenance.

Evidence card B14 — 19 Nov 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

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

Note. Paste URLs are removed; illustrates steady credential-stuffing supply during the 12 to 26 November recent window.

Held

A 19 November listing posted across two forums distributes a 1,500-line Czech mail-access file, alongside mid-November ads for a bulk IMAP/POP3/SMTP checker supporting Czech consumer webmail services.

Not established

Working credentials, unique Czech individuals, server-side mail-provider compromise or fresh capture.

Four forum observations across January, March, May and November 2026 show why raw credential lists rarely equal Czech server breaches [S1]. On **24 January**, a poster advertised `121K++ Czech Republic` credentials (`B05`), yet the thread's own download path pointed directly to `argentina.txt` , demonstrating straightforward geographic mislabelling [S1]. On **2 March**, a seller uploaded `17K (.cz)` mail-and-password lines alongside recurring monthly `1K` batches (`B07`) [S1].

On **15 May**, a poster shared 100-line URL-filtered extracts labelled for Czech telecom and streaming portals (`B06`), a hallmark of end-user infostealer logs rather than operator database breaches [S1]. Inside the recent window on **19 November**, another thread offered `1.5K Czech Mail Access` (`B14`) [S1]. Mid-November tool marketing also advertised the `Krantz Mail` automated credential checker explicitly supporting Czech consumer webmail services [S1]. Consumer platforms should respond to URL-filtered extracts and checker ads with strict login rate limits, credential-stuffing detection and compulsory MFA rather than assuming backend intrusion [S1].

4.4 Telecom bypasses, forged KYC documents and Czech strong-ID demand

CASE E

E

SMS and call spoofing routes, IMSI-catcher hardware and Czech SIM rental

Services offered

Telecommunications and SMS

Bottom line

Move authentication off SMS, verify anti-spoofing filters with carriers and warn customers that official agencies never demand payment via text links.

Evidence card B08 — 23 Jul 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

[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.

Note. Separate June Telegram posts also marketed Czech alphanumeric SMS Sender ID routes; ČTÚ previously warned that fraudsters shifted toward SMS phishing after call-spoofing filters.

Held

A multi-forum July advertisement markets global SMS and caller-ID spoofing across more than 180 destinations plus European delivery of portable false base-station hardware for cryptocurrency.

Not established

Actual delivery rates into Czech mobile networks, verified hardware supply or attribution to any specific Czech scam wave.

Evidence card B09 — 21 Nov 2026

Forum poster (alias withheld) | Forum thread | Forum | Russian

ORIGINAL

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

TRANSLATION

Rental of physical mobile-operator SIM cards for receiving SMS (MNO and MVNO: real SIMs only, we do not use VoIP or virtual PBXs). For registrations and long-term service work [...] 18+ countries [...] 30 days from USD 4.00.

Note. Service URLs and handles are removed; non-VoIP rental lines are marketed to bypass virtual-number blocks during online onboarding.

Held

A November forum advertisement offers long-term rental of non-VoIP physical SIM lines for SMS verification across more than 18 countries including Czechia, complementing earlier February Czech eSIM offers.

Not established

Czech carrier involvement, live line inventory or confirmed use in specific Czech account takeovers.

Underground telecom supply evolved in step with Czech anti-spoofing enforcement in 2026 [S1][S34][S35]. Earlier threads offered Czech eSIM profiles (`11 February`) and Czech alphanumeric SMS Sender ID routes (`6 June`) [S1]. On **23 July**, multi-forum listings promoted **180+ destination SMS and call spoofing gateways** alongside European IMSI-catcher hardware (`B08`) [S1]. Inside the recent window on **21 November**, a Russian-language thread advertised non-VoIP **physical Czech SIM rentals** (`SMS Arena`) for SMS one-time-password verification (`B09`) [S1]. These offerings align directly with the Czech Telecommunication Office (ČTÚ) warning that landline call-spoofing blocks pushed fraudsters toward smishing and SMS verification abuse [S34][S35].

CASE F

F

Custom Czech utility and payslip forgeries, EU KYC packs and turnkey nominee Czech companies

Identity verification and KYB

Services offered

Bottom line

Pair document uploads with independent registry checks, liveness controls and enhanced due diligence on newly formed Czech companies.

Fraud inputs extend well beyond stolen passwords into fabricated domestic paperwork and turnkey corporate shells, documented inline via Post Cards `B10`, `B11` and `B12` in §8.2 [S1]. On **21 August**, a forum vendor advertised **custom Czech proof-of-address bills, utility invoices and payslips** (`B10`) [S1]. On **19 August**, another offered **USD 25 EU KYC ID-and-selfie packs** including Czechia (`B11`), following **19 April** recruitment paying **USD 30** for live verification links [S1].

Earlier, on **12 January**, a Russian-language thread offered **nominee Czech sole proprietors at USD 3,500** and **nominee Czech LLCs (s.r.o.) at USD 4,900**, claiming bundled bank accounts and hardware digital-signature tokens (`B12`) [S1]. While onboarding validity is unverified, these listings show how organised fraud groups attempt to bypass Czech banking and AML controls at account creation [S1].

CASE G

G Explicit buyer demand for Czech Bank iD and MojeID plus cross-border bank-mule handovers

Demand unverified

Banking, Bank iD and MojeID

Bottom line

Add out-of-band friction to Bank iD and MojeID onboarding, monitor newly opened mule accounts for rapid cash-out and share alerts across banks.

Chapters 8 and 9 examine the banking consequence of these inputs using Post Cards `B15` and `B16` [S1]. Between **10 and 12 August 2026**, Telegram buyers explicitly requested **Czech Bank iD** access at **USD 100 per account** (echoing earlier 4 February betting-account Bank iD demand) and posted `WTB. KYC MojeID. Only Czech Republic` (`B15`) [S1].

From January through October, Russian- and Ukrainian-language Telegram brokers coordinated **bank-mule handovers across Prague, Bratislava, Warsaw and Wrocław** (`B16`) [S1]. Listings quoted **USD 170 to 700 per retail account** or **20% to 35% cash-out commissions** (specific bank names redacted) [S1]. Together, Cases F and G tie underground supply directly to the **legalizační účty** (money-mule accounts) flagged by Czech Police and the **CZK 11.8 billion** banking-fraud wave tracked by the Czech Banking Association (ČBA) [S25][S29][S30][S31].

KEY TAKEAWAYS

01

Forensic comparison of a 22 November "Year: 2026 Fresh" Czech e-shop listing against a 24 February thread showed exact schema recycling of 2025 data.

02

Mislabelled foreign combos (`argentina.txt`) and URL-filtered stealer extracts explain most Czech credential packs without establishing server breaches.

03

Underground telecom SIM rentals, forged Czech payslips, nominee LLC shells and Bank iD buyer demand directly feed domestic fraud and mule-account networks.

CHAPTER 05

Public incidents, suppliers and recent activity

05

THIS CHAPTER ANSWERS

Which publicly confirmed incidents affected Czech organisations in 2026, including 12 to 26 November?

11

public-event dossiers covering confirmed Czech disruptions and disclosures

5.1 Spring to mid-summer 2026: municipal ransomware, routers and edge bots 39

5.2 August to early November 2026: WordPress, financial subsidiaries, SaaS, PHP2Shell and OT warnings 41

5.3 Recent activity: 12 to 26 November 2026 43

CHAPTER 05

Public incidents, suppliers and recent activity

IN SHORT

Publicly confirmed 2026 Czech incidents centre on four vectors: municipal and retail ransomware, exposed web and router software, third-party suppliers and university web-to-database access. Major events hit Jemnice, Židlochovice, Náměšť nad Oslavou, Šumperk, Partners Group non-bank units, BitFaktura, Rohlík.cz, ČVUT, Univerzita Karlova, Dedoles and PRO-DOMA. Three major events arrived in 12 to 26 November, separate from a non-cyber ministry outage. Patch §12.2 flaws and audit vendor archives now.

5.1 Spring to mid-summer 2026: municipal ransomware, routers and edge bots

CASE H

H

Spring municipal cyberattack wave in Jemnice, Židlochovice and Náměšť nad Oslavou

Confirmed attacks

Regional and local administration

Bottom line

Keep immutable offline backups tested for full municipal rebuilds and migrate local-government domains out of monitoring-only or missing DMARC.

Three Moravian and Vysočina municipalities experienced disruptive cyberattacks within weeks during spring 2026, revealing how small local-government IT teams cope with ransomware [S37][S38][S39][S40]. On **9 March**, ransomware hit the municipal office in **Jemnice** (Městský úřad Jemnice), disrupting office systems and forcing gradual restoration of citizen services; Ransompedia later logged a matching **Lockbit5** entry on **6 April** [S2][S37].

Less than a week later, on **15 March**, **Deadlock** ransomware encrypted the municipal office in **Židlochovice** (Městský úřad Židlochovice) [S38][S39]. National reporting a month later detailed prolonged recovery involving cash-only counter operations and manual paperwork while systems were rebuilt [S39]. Ransompedia logged a matching **Deadlock** listing on **10 July**, mis-tagging the municipality as `medias-and-audiovisual` [S2]. Around the same period in late March and early April, a cyberattack struck **Náměšť nad Oslavou** (Městský úřad Náměšť nad Oslavou), where staff rebuilt roughly **70 workstations** cleanly from **offline backups** [S40].

CASE I

REDHEBERG VNC botnet and Czech Military Intelligence APT28 TP-Link router intervention

Official warnings

Exposed VNC and SOHO routers

Bottom line

Remove unauthenticated VNC from the public internet immediately and retire or isolate unsupported End-of-Life TP-Link routers.

Two official spring advisories underscored exposed residential, small-business and unmanaged edge devices across Czechia [S6][S7][S61][S62][S84]. In its Q1 2026 review, NÚKIB reported over **3,200 Czech devices** participating in the **REDHEBERG** botnet through internet-exposed Virtual Network Computing (VNC) services [S6].

In April 2026, FBI IC3 (`PSA260407`) and NÚKIB's Q2 overview documented widespread exploitation of legacy **TP-Link SOHO routers** (`CVE-2023-50224`) attributed by the cited agencies to Russian military intelligence (**GRU / APT28**) [S7][S61][S62][S84]. NÚKIB reported that **Czech Military Intelligence (Vojenské zpravodajství)** conducted an **active defensive intervention** to protect affected Czech routers [S7]. Because legacy TP-Link models such as End-of-Life `TL-WR841N` hardware no longer receive routine patches, replacement with supported devices and disabling internet-facing management interfaces remain the only durable controls (§12.2) [S62][S84].

CASE J

Late-July cyberattack on Městský úřad Šumperk and municipal police

Confirmed attack

Municipal administration

Bottom line

Segment municipal administrative and municipal-police networks, protect payment counters with fallback procedures and report intrusions promptly.

In **late July 2026**, a cyberattack hit the municipal office in **Šumperk** (Městský úřad Šumperk) and affected **municipal police** (městská policie) IT systems [S41]. The Police of the Czech Republic opened a formal criminal investigation [S41]. On **28 September**, the extortion label **Safepay** published a matching listing on Ransompedia, mistagging the town hall under `retail-and-commerce` [S2]. The Šumperk incident demonstrates why local public-safety and municipal-police networks must be strictly segmented from general town-hall office systems [S41].

5.2 August to early November 2026: WordPress, financial subsidiaries, SaaS, PHP2Shell and OT warnings

CASE K

K

WordPress wp2shell exploitation wave and ClickFix / PSW.Agent malware

Public websites and endpoints

Confirmed exploit

Bottom line

Patch WordPress core immediately for wp2shell flaws and block paste-and-run shell execution used in ClickFix social engineering.

During **August 2026**, mass exploitation targeted two chained WordPress core flaws known publicly as `wp2shell` [S63][S77][S78]. They combine REST API batch route confusion (`CVE-2026-63030`, CVSS 9.8) with `WP_Query` `author__not_in` SQL injection (`CVE-2026-60137`, CVSS 5.9) [S77][S78]. NÚKIB's August and Q3 summaries linked this wave to **eight revised significant Czech incidents** (nine reported initially) [S8][S15]. Both CVEs appear in CISA's KEV catalogue and pushed Intrusion to roughly two-thirds of all Q3 Czech incidents recorded by NÚKIB [S8][S77][S78].

In parallel on desktop endpoints, ESET Czechia's Q3 2026 telemetry flagged **ClickFix** lures as the top delivery path for `PSW.Agent` **infostealers** targeting Czech macOS users [S60]. These lures trick users into copying and running malicious shell commands from fake verification pages [S60]. Web teams must keep WordPress updated to `6.8.6+`, `6.9.5+` or `7.0.2+` (§12.2), while endpoint teams should restrict script execution and train staff against copy-paste prompts [S60][S63][S77][S78].

CASE L

L

Partners Group non-bank subsidiaries breach and banking-infrastructure separation

Financial advisory and insurance

Confirmed breach

Bottom line

Isolate licensed banking platforms from non-bank group IT environments and warn affected advisory clients against follow-on impersonation scams.

On **23 August 2026** (disclosed on **27 August**), a cyberattack struck four non-bank financial and insurance subsidiaries within the Czech **Partners Group** [S42][S43]. The intrusion exposed client personal data at **Partners Financial Services**, **Simplea**, **Rentea** and **Partners investiční společnost** [S42][S43]. Crucially, **Partners Banka** published an official notice confirming that its separate regulated banking infrastructure and customer accounts were **unaffected** by the intrusion [S42].

On **16 September** and again on **12 November**, **INC Ransom** listed `Partners Financial Services, a.s.` on its leak site, accounting for one of Czechia's two repeat Ransompedia entries in 2026 [S2]. Partners Banka stated that its separate banking infrastructure was unaffected [S42]. Keeping licensed banking systems and identities separate from affiliated subsidiaries limits the paths an intruder can take.

CASE M

M

BitFaktura invoicing database intrusion across Poland and Czechia

Cloud invoicing SaaS

Confirmed breach

Bottom line

Rotate exposed API keys, enforce IP allowlists on invoicing integrations and verify every supplier bank-account change by callback on a known number.

Between **27 and 28 September 2026**, an attacker held unauthorised database access for roughly **38 hours** at online invoicing provider **BitFaktura** (`bitfaktura.cz`), affecting **all accounts** across Poland and Czechia [S44] [S45]. Company notices published between **29 September and 6 October** confirmed that payment-card details were not stored in the affected database [S44]. The operator informed **CERT Polska**, Poland's data protection authority (**UODO**) and Czechia's **ÚOOÚ** [S44][S45]. Because invoicing databases hold supplier names, tax IDs and IBAN bank details for thousands of small businesses, Czech SMEs should warn finance staff against altered-IBAN invoice-redirection fraud following the breach [S44][S45].

CASE N

N

Rohlík.cz customer-support tool data breach

Online grocery retail

Confirmed breach

Bottom line

Restrict access and retention inside customer-support and AI-assistant tools and warn shoppers against targeted refund or payment lures.

On **11 October 2026**, major Czech online grocer **Rohlík.cz** disclosed unauthorised access to a **customer-support tool** exposing support chats, call transcripts and customer emails spanning **April to October 2026** [S46][S47]. The company confirmed that **passwords and payment-card data were unaffected** and notified both **ÚOOÚ** and **NÚKIB** [S46][S47]. Even without credentials or card numbers, six months of authentic delivery complaints and refund conversations give fraudsters realistic pretexts for targeted smishing and phone scams [S46][S47].

CASE O

October PHP2Shell wave across Úřad vlády ČR, ČHMÚ and ČVUT

Shutdown & attack

Government web and academia

Bottom line

Pre-authorise rapid precautionary web isolation ahead of runtime patches and upgrade PHP installations to current November security releases.

On **21 October 2026**, two critical PHP remote code execution flaws dubbed **PHP2Shell** were disclosed (`CVE-2026-109618`, CVSS 9.8, and `CVE-2026-109619`, CVSS 8.1) [S74][S75]. They caused immediate disruption across Czech public and academic web portals [S17][S48][S50]. Following NÚKIB's emergency alert, the **Office of the Government (Úřad vlády ČR)** performed a roughly **two-hour precautionary website shutdown** with no intrusion confirmed, while the **Czech Hydrometeorological Institute (ČHMÚ)** restricted affected online services [S48] [S50].

At **Czech Technical University in Prague (ČVUT)**, defenders halted an **active exploitation attempt** and carried out a partial system shutdown to contain exposure [S49]. On **19 November**, PHP disclosed a separate critical session-serializer mismatch flaw (`CVE-2026-115560` / `GHSA-658j-r8rw-q6mx`, CVSS 4.0 score 9.2) [S65][S76]. The **19 November releases** (`8.5.13`, `8.4.28`, `8.3.37`, `8.2.36` or later) are therefore the mandatory current remediation baseline (§12.2) [S64][S65].

Separately, an early-November European cyberattack wave hit internet-exposed **grocery refrigeration controllers** [S51]. On **11 November**, NÚKIB issued a preventive warning urging Czech operators to isolate industrial cooling and building-automation controllers from the public internet, with **no confirmed Czech retail victim** reported by cut-off [S51]. Similarly, global exploitation of **Citrix NetScaler ADC and Gateway** zero-days (`CVE-2026-88771`, `CVE-2026-88772`, plus 12 November `CTX697305` / `CVE-2026-120868`) had no publicly named Czech victim before cut-off [S79][S80][S81]. Both remain urgent patching priorities in §12.2 [S79][S80][S81].

5.3 Recent activity: 12 to 26 November 2026

This subsection covers strictly the **15-day recent window from 12 to 26 November 2026** and does not extrapolate those counts to longer periods [S1][S2]. Within those fifteen days, Brandefense observed **1,771 Czechia-tagged underground posts** (including **53 forum posts**, not all of them Czech-targeted) [S1]. Ransompedia logged **three Czechia-labelled listings** in the same window: the 12 November repeat `INC Ransom` entry for `Partners Financial Services` plus two unconfirmed entries [S2]. Forum activity included `19 November 1.5K mail access`, `21 November SMS Arena Czech SIMs` and `22 November` recycled `~105K` e-shop listings [S1]. Three major publicly confirmed Czech incidents also unfolded (`Cases P, Q and R`) [S52][S55][S57].

CASE P

P

Univerzita Karlova (Charles University) Student Information System breach

Confirmed breach

Higher education

Bottom line

Isolate web applications from central student-information databases, enforce least privilege on database links and separate cyber notices from cloud outages.

On **13 November 2026**, an attacker exploited a vulnerability in a web application at **Univerzita Karlova (Charles University)** to access and download data from the central **Student Information System (SIS)**, including personal data [S52][S53][S54]. As a precaution, the university prompted roughly **55,000 students and staff** to change their Central Authentication Service (**CAS**) passwords [S53][S54]. Official university follow-up notices clarified that there was **no evidence of widespread CAS credential theft**, while the Police of the Czech Republic and NÚKIB opened investigations [S52][S53][S54].

Crisis communicators should note a key same-day distinction on **13 November** [S54]. An IT outage hit the Czech ministries of **Finance, Transport and Education**, and **Microsoft Czechia confirmed an internal technical failure rather than a cyberattack** [S54]. Separating parallel technical outages from verified intrusions prevents public confusion and preserves investigative focus [S54].

CASE Q

Q

Dedoles legacy e-shop breach via Slovak IT supplier ui42

Supplier breach

Cross-border e-commerce supplier

Bottom line

Decommission legacy e-shop backups promptly, require MFA for every external IT agency account and monitor cross-border Czech-Slovak supplier access.

Between **20 and 23 November 2026**, Slovak apparel retailer **Dedoles** (widely active across Czechia) disclosed a third-party data breach [S55][S56]. An attacker used stolen employee credentials at Slovak IT supplier `ui42` to copy a **legacy e-shop database** backup [S55][S56]. The stolen archive covered customer orders and invoicing records from **September 2021 to June 2026** (names, contact details, addresses, purchased items, invoice numbers and payment methods) across Czech and Slovak shoppers [S55][S56]. Dedoles stated that its current e-shop (migrated after July 2026), customer passwords and payment cards were unaffected, revoked supplier access and warned shoppers against order-themed phishing [S55][S56].

CASE R

R

PRO-DOMA building-materials ransomware attack and tape-backup recovery

Building-materials retail

Ransomware attack

Bottom line

Keep offline tape or immutable backups ready for clean infrastructure rebuilds, enforce VPN MFA and separate work laptops from home networks.

Overnight on **24 to 25 November 2026**, ransomware struck major Czech building-materials distributor **PRO-DOMA**, forcing all **173 Czech branches** onto paper-and-pencil sales fallback [S57]. According to company statements reported by Seznam Zprávy, management **refused to negotiate** and confirmed that business data survived intact on **magnetic-tape backups** [S57]. The firm began a clean **10 to 14 day** infrastructure rebuild [S57]. The company's chief executive attributed the attack publicly to a Russian group called **Gold Ogre / Aurora** and cited a workstation or home-device link as a suspected entry path [S57]. Those statements are recorded here strictly as the company's own disclosure rather than an independent agency attribution [S57].

KEY TAKEAWAYS

01

Náměšť nad Oslavou and PRO-DOMA recovered from offline or tape backups, and Židlochovice and PRO-DOMA kept serving customers on manual fallback.

02

Web-application and edge flaws (WordPress wp2shell, PHP2Shell, Charles University SIS) plus third-party platforms (BitFaktura, Rohlík.cz, Dedoles/u142) dominated 2026 data exposures.

03

Separate confirmed cyber incidents cleanly from parallel technical outages, as demonstrated on 13 November across Charles University and three Czech ministries.

CHAPTER 06

Disruption, hacktivism and claim versus reality

06

THIS CHAPTER ANSWERS

How should Czech defenders distinguish hacktivist claims from verified service impact?

0 and 4

DDoS incidents logged by NÚKIB in September and October despite loud Telegram waves

6.1 Chronology of 2026 Czech disruption and resilience milestones 47

6.2 Hacktivist DDoS tempo and unverified industrial claims 48

6.3 Claim versus official record 48

CHAPTER 06

Disruption, hacktivism and claim versus reality

IN SHORT

Hacktivist channels that NÚKIB describes as pro-Russian (`NoName057(16)` , `Server Killers` , `Z-Pentest Alliance`) repeatedly claimed Czech government takedowns and industrial-control takeovers in 2026 around policy announcements and ahead of the October elections. Yet NÚKIB recorded zero DDoS incidents in September and four in October, and independent checks found no evidence for sweeping camera and heating-control claims. Verify every claim against owned uptime telemetry and publish calm status updates without repeating actor rhetoric.

6.1 Chronology of 2026 Czech disruption and resilience milestones

7 Jan 2026	Czech State Security Council publishes statement on the international ammunition initiative [S36]
9 Jan 2026	Bilingual `Server Killers` Telegram post threatens Czech public infrastructure; NÚKIB logs January DDoS wave [S1][S9]
9 Mar 2026	Spring municipal cyberattacks begin at Městský úřad Jemnice (ransomware), followed by Židlochovice (15 Mar, ransomware) and Náměšť nad Oslavou [S37][S38][S40]
7 Apr 2026	FBI IC3 and NÚKIB warn on APT28 TP-Link router exploitation (`CVE-2023-50224`); Czech Military Intelligence intervenes actively [S7][S61]
28 Jul 2026	Late-July cyberattack disrupts Městský úřad Šumperk and municipal police systems [S41]
15 Aug 2026	WordPress `wp2shell` (`CVE-2026-63030` , `CVE-2026-60137`) drives 8 revised significant Czech incidents in August [S8][S15]
23 Aug 2026	Partners Group non-bank subsidiaries hit by cyberattack; Partners Banka confirms separate banking systems unaffected [S42][S43]
28 Sep 2026	`NoName057(16)` runs `#OpCzechRepublic` / `#FuckEastwood` DDoS Telegram wave through 4 October in the run-up to the 9–10 October elections [S1][S67]
21 Oct 2026	PHP2Shell (`CVE-2026-109618` , `CVE-2026-109619`) triggers Úřad vlády ČR precautionary shutdown, ČHMÚ restrictions and ČVUT active-attack response [S48][S49][S50]
11 Nov 2026	NÚKIB issues preventive OT warning on exposed refrigeration controllers; no Czech retail victim confirmed at cut-off [S51]
13 Nov 2026	Univerzita Karlova discloses SIS web-app breach; same-day ministry outage confirmed as non-cyber Microsoft technical failure [S52][S54]
24 Nov 2026	CZ.NIC and NÚKIB sign National CSIRT public-law contract; PRO-DOMA ransomware hits overnight across 173 branches [S24][S57]

6.2 Hacktivist DDoS tempo and unverified industrial claims

In **July 2025**, coordinated international law-enforcement action (**Operation Eastwood**, led by Europol and Eurojust with Czech participation) disrupted infrastructure linked to `NoName057(16)` [S5][S85]. Hacktivist Telegram activity nonetheless persisted in reduced, episodic bursts during 2026 [S1][S9][S17].

On **9 January 2026**, two days after the State Security Council statement on the ammunition initiative, a bilingual English and Czech `Server Killers` Telegram post threatened Czech public infrastructure [S1][S36]. That matched NÚKIB's January report naming both `NoName057(16)` and `ServerKillers` [S9]. Later, between **28 September and 4 October**, `NoName057(16)` channels pushed multi-language `#OpCzechRepublic` and `#FuckEastwood` target lists in the run-up to the **9–10 October** municipal and Senate elections [S1][S67]. Those posts claimed disruption across Czech public and transport sites [S1]. Across that entire period, NÚKIB recorded **zero DDoS incidents in September** and **four in October** among incidents reported to it, far fewer than the Telegram claims implied [S16][S17].

Separately, Telegram channels linked to `Z-Pentest Alliance` and peer collectives posted unverified claims alleging access to Czech security cameras and heating equipment [S1][S58]. Specific unverified posts claimed an 850 kW thermal boiler (17–18 January), a heating station (2 May) and a wood-drying chamber (26 October; all unverified facility names withheld) [S1]. Following an October media wave, `Lupa.cz` cited Check Point's assessment that no evidence supported claims of thousands of breached Czech cameras or widespread heating takeovers [S58]. That finding echoes NÚKIB's joint international warning on hacktivist OT exaggeration [S19].

6.3 Claim versus official record

Czech defenders face recurring pressure from dramatic Telegram posts, same-day outages and inflated leak-site claims. The table below pairs prominent 2026 claims against the verified record.

Claim or public perception	Established record	Defensive discipline
`NoName057(16)` `#OpCzechRepublic` / `#FuckEastwood` Telegram posts claim sweeping Czech public-site takedowns (28 Sep–4 Oct) [S1]	NÚKIB recorded **0 DDoS incidents in September** and **4 in October** among reported incidents; no systemic outage was reported [S16][S17]	Measure uptime from owned monitoring and upstream scrubbing logs; publish factual status updates without quoting actor slogans
`Z-Pentest Alliance` and Telegram channels claim takeovers of thousands of Czech cameras and heating controllers [S1][S58]	Unverified claims; independent technical review found no confirmation of mass Czech camera or heating-system takeover, though exposed OT controllers still require isolation [S19][S51][S58]	Inventory and remove exposed HMI, PLC and refrigeration interfaces from the public internet instead of reacting to Telegram screenshots
Same-day 13 November outages at three Czech ministries and Charles University perceived as one coordinated cyberattack [S54]	Charles University confirmed an SIS web-application data breach, whereas Microsoft Czechia confirmed an internal non-cyber technical cause for the ministry outage [S52][S54]	Verify root cause before linking parallel outages in crisis briefings or statutory notifications

Claim or public perception	Established record	Defensive discipline
October website downtime at the Office of the Government (Úřad vlády ČR) perceived as an intrusion [S48]	Confirmed as a roughly two-hour precautionary shutdown to mitigate PHP2Shell (`CVE-2026-109618` , `CVE-2026-109619`) ahead of patching, with no breach reported [S48][S50]	Pre-authorise preventive DMZ shutdowns and state plainly when downtime is precautionary
22 November forum post advertises a ~105K Czech e-shop database as "Year: 2026 Fresh" [S1]	Schema and timestamp comparison matches a 24 February listing whose records ended 25 November 2025; underlying target unconfirmed [S1]	Compare column names and latest timestamps against prior archives before declaring a new breach

KEY TAKEAWAYS

01

NÚKIB logged 0 DDoS incidents in September and 4 in October despite intense #OpCzechRepublic Telegram messaging.

02

Unverified camera and heating-controller claims lacked independent proof, yet NÚKIB's 11 November refrigeration warning underscores why internet-exposed OT must still be removed.

03

Separate confirmed intrusions from precautionary shutdowns and non-cyber technical failures in every public notice.

CHAPTER 07

Ransomware, espionage advisories and threat profiles

07

THIS CHAPTER ANSWERS

Who is claiming Czech targets, and what separates an extortion label from a state advisory?

50

Czechia-labelled ransomware listings across 20 claimant labels

7.1 Regional ransomware listings and monthly concentration 51

7.2 Threat network and profiled extortion and hacktivist actors 53

7.3 State-linked espionage advisories targeting Czechia 58

CHAPTER 07

Ransomware, espionage advisories and threat profiles

IN SHORT

Ransompedia logged 50 Czechia-labelled extortion listings between 1 January and 26 November 2026, nearly double the 27 recorded in full-year 2025, with a peak of 13 in July. Five listings, covering four confirmed public Czech cases (Jemnice, Židlochovice, Partners Financial Services twice and Šumperk), match public reporting, leaving 45 unverified claims. Separately, NÚKIB and allied advisories document Russian and PRC-linked espionage campaigns exploiting known bugs and weak authentication. Harden backups, patch §12.2 flaws and verify every leak-site claim internally.

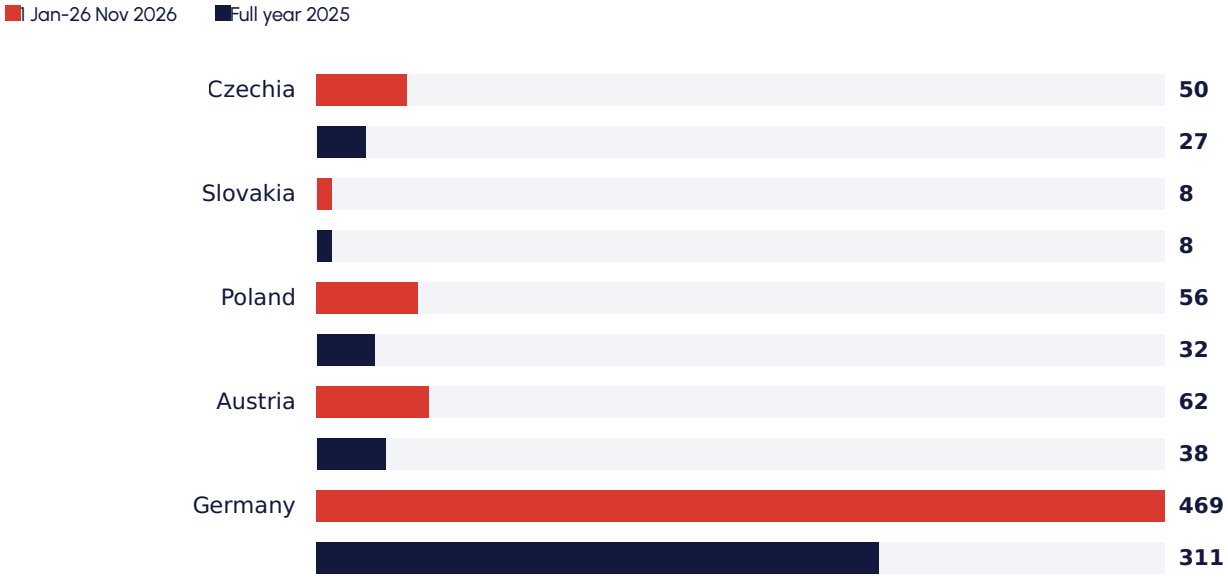
7.1 Regional ransomware listings and monthly concentration

Between **1 January and 26 November 2026**, Ransompedia recorded **50 Czechia-labelled extortion listings** across **20 claimant labels**, up from **27 listings** across full-year 2025 (**119** all-time) [S2]. That rise aligns directionally with ESET Czechia's Q1 2026 press review noting a 100% year-on-year increase to 12 recorded Czech ransomware victims in Q1 alone [S59]. Monthly Ransompedia volume ran: January **3**, February **3**, March **5**, April **5**, May **1**, June **2**, **July 13**, August **6**, September **5**, October **4** and partial November **3** [S2]. The three November entries comprise one repeat confirmed listing and two unconfirmed entries [S2].

Two repeat listings reduce the 50 entries to **at most 48 distinct claimed entities** [S2]. Specifically, `Partners Financial Services, a.s.` appeared twice under **INC Ransom** (`16 September` and `12 November`), and one unconfirmed entity (withheld) appeared twice under two separate claimant labels [S2][S42]. Across all 50 listings, only **five entries** (four confirmed public Czech cases in Chapter 5) match public reporting [S2].

Those five entries cover **Městský úřad Jemnice** (`Lockbit5`, 6 April), **Městský úřad Židlochovice** (`Deadlock`, 10 July), **Partners Financial Services** (`INC Ransom`, 16 September and 12 November) and **Městský úřad Šumperk** (`Safepay`, 28 September) [S2][S37][S38][S41][S42]. The remaining **45 entries** (at most **44 distinct entities**) have no public Czech confirmation and remain strictly unverified and withheld [S2]. Sector tagging on leak sites is also error-prone: both Židlochovice (`medias-and-audiovisual`) and Šumperk (`retail-and-commerce`) were mis-tagged by extortion portals [S2].

Czechia's 50 ransomware listings nearly double 2025 totals and trail Poland, Austria and Germany



Source: Brandefense Ransompedia, 1 January-26 November 2026 versus full-year 2025 [S2]. Unequal periods; country-labelled claims, not unique victims, confirmed intrusions or a national security ranking.

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

Placed alongside its four border neighbours over the same 2026 window (versus full-year 2025), Czechia sits between Slovakia and its larger or wealthier peers [S2]:

Country	2026 window listings (1 Jan–26 Nov)	Full-year 2025 listings	Leading 2026 claimant labels	Sources
Czechia (CZ)	**50**	**27**	The Gentlemen (16), Titan (4), Krybit (3), Lockbit5 (3), AKIRA (3), Qilin (3), Deadlock (3), INC Ransom (2), Safe-pay (2)	[S2]
Slovakia (SK)	8	8	Qilin (2), APT73 (2), The Gentlemen (1), Safepay (1), Clop (1), INC Ransom (1)	[S2]
Poland (PL)	56	32	The Gentlemen (19), Deadlock (5), Coin-basecartel (4), Nova (4), Qilin (3)	[S2]
Austria (AT)	62	38	The Gentlemen (11), Qilin (9), Lockbit5 (8), Krybit (4), Payload (4)	[S2]
Germany (DE)	469	311	Qilin (63), Safepay (58), The Gentlemen (48), AKIRA (29), Payload (20)	[S2]

Notice that **The Gentlemen** led Czechia (**16 listings**, 32%), Poland (**19**) and Austria (**11**) while sitting third in Germany (**48**), reflecting a regional Central European extortion surge rather than an isolated domestic anomaly [S2]. Eleven further labels appeared once each in Czechia during 2026 (full label counts in the c08 chart data) [S2]. Separately, PRO-DOMA's overnight 24–25 November ransomware disruption (`Case R`) did not appear on Ransompedia by our 26 November cut-off, although the company publicly attributed the attack to a named Russian group (§5.3) [S2][S57].

7.2 Threat network and profiled extortion and hacktivist actors

The network diagram and group cards below distinguish financially motivated ransomware extortion labels, hacktivist disruption channels and state-attributed espionage clusters active around Czechia in 2026.

Own post Relay Official statement Public reporting Our observation

The Gentlemen

Own data
16 listings, S2 ↓

Czechia-labelled listings (50)

Own data
2 repeat listings, S2 ↑

INC Ransom

Deadlock

Own data
3 listings (incl. confirmed municipal case), S2, S38 ↓

Czechia-labelled listings (50)

Own data
3 listings (incl. confirmed municipal case), S2, S37 ↑

Lockbit5

NoName057(16) & ServerKillers

Official
Jan 2026 DDoS wave & 42 incidents since 2023, S9, S19 ↑

Official Czech & allied advisories

Official
Dec 2025 & Q1 2026 VNC/OT warnings, S6, S19 ↓

Z-Pentest Alliance

GRU / APT28 advisory

Official
Apr 2026 TP-Link router intervention, S7, S61 ↑

Official Czech & allied advisories

Official
Q3 2026 Zimbra & Signal/Device Code warnings, S8, S18 ↓

LAUNDRY BEAR & STORM-2372

SparkyCarp & PRC advisories

Official
Q2-Q3 2026 European Values & BlueMoon advisories, S7, S8 ↑

Official Czech & allied advisories

The Gentlemen

Thegentlemen (label in observed listings)

Ransomware/extortion listing label | No state attribution established here

IN CZECHIA, 2026

2026 window

16 Czechia-labelled listings (32.0% of 50), Jan-Nov 2026, S2

1 Apr 2026

Named by ESET Czechia among top three active RaaS groups targeting Czechia, S59

CLAIMED TARGETS

Czechia-labelled entries across several sectors (all 16 unconfirmed; identities, sectors and dates withheld)

SEEN IN PUBLIC REPORTING

[S2] 16 Czechia-labelled listings in Ransompedia across 2026

[S59] ESET Czechia Q1 2026 ransomware release naming Gentlemen, Akira and Qilin

OUR ASSESSMENT

The Gentlemen is the single largest claimant label on Czechia-labelled Ransompedia entries in 2026 (16 of 50). A leak-site entry verifies an extortion claim rather than confirmed encryption, data loss or accurate sector tagging.

CONFIDENCE

High for the recorded count and ESET reporting; individual unconfirmed claims remain unverified

INC Ransom

Label in observed listings

Ransomware/extortion listing label | No state attribution established here

IN CZECHIA, 2026

Sep & Nov 2026

2 repeat Czechia-labelled listings (16 Sep and 12 Nov) matching confirmed non-bank financial subsidiary Partners Financial Services, S2, S42, S43

CLAIMED TARGETS

Non-bank financial advisory subsidiary (Partners Financial Services confirmed an August cyberattack; Partners Banka explicitly unaffected)

SEEN IN PUBLIC REPORTING

[S2] 2 repeat listings recorded in Ransompedia (16 Sep and 12 Nov)

[S42] Partners Banka official statement confirming non-bank subsidiaries affected

[S43] Novinky.cz national press reporting on Partners Group breach

OUR ASSESSMENT

INC Ransom's September and 12 November listings illustrate how repeat postings inflate raw country counts while echoing a confirmed August incident. Partners Group confirmed personal-data access at non-bank subsidiaries and stressed that Partners Banka was unaffected.

CONFIDENCE

High for the recorded repeat count and official company disclosure; scope of attacker-held files remains unverified

Deadlock

Label in observed listings

Ransomware/extortion listing label | No state attribution established here

IN CZECHIA, 2026

15 Mar 2026

Confirmed Deadlock ransomware attack disrupted Městský úřad Židlochovice, S38, S39

2026 window

3 Czechia-labelled listings in Ransompedia, including the confirmed Židlochovice listing, S2

CLAIMED TARGETS

Confirmed municipal town hall (Židlochovice) plus two unconfirmed entries (identities, sectors and dates withheld)

SEEN IN PUBLIC REPORTING

[S2] 3 Czechia-labelled entries in Ransompedia across 2026

[S38] Novinky.cz report confirming Deadlock ransomware at Židlochovice town hall

[S39] Seznam Zprávy follow-up on month-long cash-only recovery

OUR ASSESSMENT

Židlochovice's March confirmation and July leak-site entry demonstrate multi-month lag between operational encryption and public extortion posting, as well as noisy feed industry tags (the town hall was tagged under media).

CONFIDENCE
High for the confirmed Židlochovice case and recorded count; other entries remain unverified

Lockbit5

Label in observed listings

Ransomware/extortion listing label | No state attribution established here

IN CZECHIA, 2026

9 Mar 2026
Confirmed ransomware attack on Městský úřad Jemnice; listed 6 April under Lockbit5, S2, S37

2026 window
3 Czechia-labelled entries in Ransompedia, including the confirmed Jemnice listing, S2

CLAIMED TARGETS

Confirmed municipal town hall (Jemnice) plus two unconfirmed entries (identities, sectors and dates withheld)

SEEN IN PUBLIC REPORTING

[S2] 3 Czechia-labelled entries in Ransompedia

[S37] Novinky.cz report confirming Jemnice town hall ransomware attack

OUR ASSESSMENT

Alongside Deadlock and Safepay (which listed Šumperk after its confirmed July intrusion), Lockbit5 highlights sustained criminal ransomware pressure on Czech municipalities that often operate under the lower-obligation cybersecurity tier.

CONFIDENCE
High for the confirmed Jemnice case and recorded count; other entries remain unverified

NoName057(16) and ServerKillers

DDoSia Project (Telegram channel label)

Hacktivist DDoS collectives | Described by NÚKIB and Europol as pro-Russian hacktivist groups

IN CZECHIA, 2026

Jan 2026
Named by NÚKIB as primary drivers of January's 32-incident spike (~half DDoS), S6, S9

CLAIMED TARGETS

Czech government portals, public-procurement platforms, regional transport, energy and logistics websites

9 Jan 2026

Server Killers posted bilingual EN/CS threat against Czech government sites referencing ammunition deliveries, S1

Sep-Oct 2026

Multi-language DDoS claim wave (#OpCzechRepublic, #FuckEastwood), while NÚKIB logged 0 DDoS in Sep and 4 in Oct, S1, S16, S17

SEEN IN PUBLIC REPORTING

[S1] Observed Telegram threat and check-host claim posts (Jan, Mar, Sep-Oct)

[S9] NÚKIB January 2026 incident report naming NoName057(16) and ServerKillers

[S19] NÚKIB Dec 2025 warning citing 42 NoName057(16) Czech incidents since 2023

[S85] ČT24 report on July 2025 Europol/Eurojust Operation Eastwood disruption

OUR ASSESSMENT

Despite July 2025 international disruption under Operation Eastwood (with Czech participation), NoName057(16) and ServerKillers drove a January 2026 DDoS peak before fading in NÚKIB's reported statistics. Late-September Telegram claims far exceeded DDoS incidents reported to NÚKIB.

CONFIDENCE

High for NÚKIB statistics and observed Telegram posts; individual unconfirmed website claims remain unverified

Z-Pentest Alliance

Z-Alliance (Telegram channel label)

Hacktivist OT intrusion claim group | Described by NÚKIB and FBI as a pro-Russian hacktivist group targeting exposed OT

IN CZECHIA, 2026

Jan, May & Oct 2026

Unverified Telegram claims of access to Czech thermal, boiler, district-heating and wood-drying HMI/SCADA controls, S1

Q1 2026

NÚKIB warned of hacktivists abusing weak or unauthenticated internet-exposed VNC on PLCs, noting minimal impact on non-regulated entities, S6

CLAIMED TARGETS

Poorly secured, internet-exposed VNC and HMI interfaces on small heating, water and industrial facilities

SEEN IN PUBLIC REPORTING

[S1] Observed Telegram OT claim posts (Jan, May, Oct 2026)

[S6] NÚKIB Q1 2026 Quarterly report on VNC/PLC exposure

[S19] NÚKIB and FBI joint warning naming Z-Pentest, CARR and NoName057(16)

OUR ASSESSMENT

Observed Telegram claims in January, May and October echo NÚKIB's warning on exposed VNC interfaces rather than establishing major infrastructure outages. Removing VNC from the public internet eliminates the primary entry path.

CONFIDENCE

High for official warnings and observed claims; individual facility claims remain unverified

7.3 State-linked espionage advisories targeting Czechia

Every state attribution in this section is stated strictly as the attribution of the cited official agency. Across its 2026 quarterly reports and its **20 October 2026 Threat Analysis**, NÚKIB highlighted a recurring operational pattern [S6] [S7][S8][S18]. State-sponsored actors targeting Czech ministries, civil-society groups and private firms blend selective espionage tooling with routine exploitation of known bugs, weak passwords and phishing [S18]. Many intrusions are preventable through basic hygiene [S18].

Russian state-sponsored activity (per NÚKIB and FBI IC3). In Q1 2026, NÚKIB tracked **APT28** (`Operation Neusploit`) abusing Microsoft Office security-feature bypass `CVE-2026-21509` (CVSS 7.8, CISA KEV) [S6][S18] [S82]. In April, FBI IC3 (`PSA260407`) and NÚKIB Q2 documented GRU / **APT28** exploitation of legacy **TP-Link SOHO routers** (`CVE-2023-50224`), met by active defensive intervention from Czech Military Intelligence [S7][S61][S62] [S84]. Across Q3 and the 20 October analysis, NÚKIB also highlighted **APT28** (`HOOKEDGE`) and **STORM-2372** (targeting Signal accounts and Microsoft 365 Device Code Flow) [S8][S18]. The same advisories tracked **LAUNDRY BEAR** exploiting Zimbra Collaboration Classic UI stored XSS `CVE-2025-66376` (CVSS 6.1/7.2, CISA KEV) [S8][S18] [S83].

PRC-linked espionage and router backdoors (per NÚKIB). Czechia's May 2025 attribution of the 2022–2024 Ministry of Foreign Affairs unclassified-network intrusion to **APT31** serves strictly as pre-2026 context [S5]. Within 2026, NÚKIB Q2 documented **SparkyCarp** phishing against Czech think tank **European Values (Evropské hodnoty)**, linking the campaign to broader collection aimed at **Taiwan** (no individual staff named) [S7]. In Q3 2026, NÚKIB further noted the **BlueMoon** browser and Windows exploit kit associated with **APT31** and three additional PRC-linked actors [S8]. The same report noted firmware backdoors affecting **Tenda** routers (reported by CERT/CC) and **Zbt-link** (`ENDLESSDOORS`) devices [S8].

GRU / APT28 (agency advisories)

Fancy Bear, Forest Blizzard, Sofacy (agency labels)

State-attributed espionage actor (official advisories) | Attributed by FBI, NÚKIB and Czech Military Intelligence to Russian military intelligence (GRU)

IN CZECHIA, 2026

Q1 2026

NÚKIB Q1 report highlighted Operation Neusploit (CVE-2026-21509) against European targets including Slovakia and Poland, S6

Apr 2026

Czech Military Intelligence actively intervened to secure exploited TP-Link routers (CVE-2023-50224), S7, S61

Q3 2026

NÚKIB Q3 report highlighted HOOKEDGE backdoor against European diplomatic targets (Recorded Future medium confidence), S8

CLAIMED TARGETS

SOHO routers (CVE-2023-50224), Microsoft Office users (CVE-2026-21509), government, military and critical-infrastructure personnel

SEEN IN PUBLIC REPORTING

[S6] NÚKIB Q1 2026 Quarterly report (Operation Neusploit)

[S7] NÚKIB Q2 2026 Quarterly report (Czech Military Intelligence active intervention)

[S8] NÚKIB Q3 2026 Quarterly report (HOOKEDGE backdoor)

[S61] FBI IC3 PSA260407 router advisory

[S84] NVD entry for CVE-2023-50224

OUR ASSESSMENT

Czech Military Intelligence's active remediation of exploited TP-Link SOHO routers inside Czechia makes the April GRU/APT28 advisory directly operational for Czech organisations. All state attributions remain strictly the cited agencies' assessments.

CONFIDENCE

High for official agency advisories; no independent operator attribution or Czech victim count

LAUNDRY BEAR and STORM-2372 (NÚKIB Q3 advisories)

Russia-linked espionage clusters (agency labels)

State-attributed espionage clusters (official advisories) | Attributed by NÚKIB and international partners to actors linked to the Russian Federation

IN CZECHIA, 2026

Q3 2026

NÚKIB joined international warning on LAUNDRY BEAR exploiting Zimbra Collaboration Suite (CVE-2025-66376) since at least July 2025, S8, S18

Q3 2026

NÚKIB warned of STORM-2372 Signal phishing and Microsoft Entra ID Device Code Flow abuse against officials and security personnel, S8

CLAIMED TARGETS

Government institutions, defence industry, energy, media, education, NGOs and officials using Signal, Microsoft 365 or Zimbra

SEEN IN PUBLIC REPORTING

[S8] NÚKIB Q3 2026 Quarterly Threat Report (Signal, Device Code Flow, Zimbra)

[S18] NÚKIB Oct 2026 Threat Analysis on Russian state-sponsored actors

[S83] NVD entry for CVE-2025-66376

OUR ASSESSMENT

NÚKIB's Q3 report and October Threat Analysis emphasise that state-attributed espionage against Czech and NATO targets relies heavily on unpatched webmail, social engineering on Signal and OAuth device-code abuse rather than exotic zero-days.

CONFIDENCE

High for published NÚKIB advisories; no Czech victim census published

SparkyCarp and PRC-linked advisories (incl. historical APT31)

UNK_SparkyCarp, APT31 (agency labels)

State-attributed espionage advisories | Attributed by NÚKIB and Czech authorities to actors linked to the People's Republic of China

CLAIMED TARGETS

Czech think tanks, NGOs, foreign-policy institutions and internet-facing browser/edge software

IN CZECHIA, 2026

Q2 2026

NÚKIB reported SparkyCarp credential-phishing attempt against Czech think tank European Values (linked by NÚKIB to a wider campaign targeting Taiwan), S7

Q3 2026

NÚKIB highlighted BlueMoon Chrome/Windows exploit kit shared by at least four PRC-linked actors including APT31, S8

May 2025 context

Historical Czech state attribution of APT31 for the 2022-2024 Ministry of Foreign Affairs unclassified-network intrusion (pre-2026 context), S5

SEEN IN PUBLIC REPORTING

[S5] NÚKIB 2025 Annual Report (historical May 2025 APT31 attribution)

[S7] NÚKIB Q2 2026 Quarterly report (SparkyCarp targeting European Values)

[S8] NÚKIB Q3 2026 Quarterly report (BlueMoon exploit kit and Tenda/Zbtlink router backdoors)

OUR ASSESSMENT

NÚKIB's Q2 and Q3 2026 bulletins report PRC-linked phishing against a Czech policy organisation alongside browser patch-gap exploitation and router firmware backdoors. The 2022-2024 MZV intrusion belongs to pre-2026 history, not 2026 counts.

CONFIDENCE

High for official NÚKIB reporting; state attributions remain strictly the issuing authorities' assessments

KEY TAKEAWAYS

01

Czechia's 50 Ransompedia listings nearly doubled 2025's count of 27, led by The Gentlemen (16), yet 45 of 50 claims remain unverified.

02

Five entries covering four confirmed public Czech incidents matched Ransompedia listings, two with misassigned sector labels.

03

NÚKIB and FBI IC3 advisories indicate that many state-attributed intrusions rely on known Office, Zimbra and router flaws and Device Code Flow abuse, so patching and blocking them closes common entry paths.

CHAPTER 08

Fraud, identity abuse and secondary harm

THIS CHAPTER ANSWERS

How do leaked personal details and underground services fuel Czechia's fraud economy?

CZK 11.8B

attempted Czech banking fraud across 75,637 attacks in Q1 to Q3 2026

8.1 National digital-fraud scale and shifting attacker tactics 63

8.2 Forged Czech documents, KYC kits and nominee company shells 63

8.3 Payment-card material: a narrow observation 66

8.4 Secondary harm after legitimate Czech data breaches 66

CHAPTER 08

Fraud, identity abuse and secondary harm

IN SHORT

Consumer and SME cyber fraud is Czechia's highest-volume financial threat in 2026. Czech police logged 21,137 cybercrimes in 2025 (+14.3%) and a record 2,533 cases in March 2026. Meanwhile, Czech banks blocked 81% of CZK 11.8 billion in Q1–Q3 attempted fraud yet saw clients lose CZK 2.2 billion. Underground sellers supply forged payslips, KYC selfies, nominee companies and physical SIMs while real breaches feed follow-on scams. Treat every customer breach as a fraud trigger and harden onboarding checks.

8.1 National digital-fraud scale and shifting attacker tactics

Official Czech crime, banking and telecom statistics paint a consistent picture of rising social engineering paired with rapid channel adaptation. In 2025, the Ministry of the Interior recorded **21,137 cybercrimes** (+2,642 or **+14.3%** year on year), rising to **12.4%** of all crime even as overall recorded crime dropped 1.9% [S25]. Clearance stood at just **15.1%**, reflecting cross-border infrastructure and rapid money-mule cash-out [S25]. In **March 2026**, Czech police logged an all-time monthly record of **2,533 cybercrime cases** (+37% year on year), with fake-banker and fake-police voice scams alone costing victims **CZK 322 million** across early 2026 [S26].

Banking-sector figures confirm both high defensive stop rates and heavy residual losses. Across **Q1 to Q3 2026**, Czech Banking Association (ČBA) data reported **75,637 attacks** (+7,611 year on year) attempting to steal **CZK 11.8 billion** [S29][S30]. Banks protected **CZK 9.6 billion (81%)**, while clients still lost **CZK 2.2 billion** [S29][S30]. The average loss stood at **CZK 29,266** per successful scam [S30]. ČBA and Ipsos testing placed Czechia's national Cybersecurity Index at **62** overall and **59** among adults aged 18 to 34 [S30]. Digital fluency alone does not immunise younger users against urgent social engineering [S30].

Regulatory telecom interventions reshaped attacker delivery channels across 2025 and 2026. The Czech Telecommunication Office (ČTÚ) introduced landline anti-spoofing rules, and a July 2025 Electronic Communications Act amendment empowered operators to block spoofed foreign calls carrying Czech prefixes [S34][S35]. Together, operators now filter **millions of fraudulent call attempts every month** [S34][S35].

In response, ČTÚ, NÚKIB, Bank iD and Portál veřejné správy warned of a sharp shift toward **smishing**, phishing emails and fake Portál občana logins [S7][S31][S32][S34]. Campaigns frequently spoof Czech Police (using `.cfd`, `.bond` and `.xyz` domains), tax refunds, postal deliveries and bank alerts [S7][S32]. Separately, ÚOOÚ recorded **1,430 spam complaints** and imposed **CZK 12.1 million** in direct-marketing fines in 2025 [S33].

8.2 Forged Czech documents, KYC kits and nominee company shells

Underground listings observed across 2026 supply the exact paperwork and corporate wrappers needed to bypass automated remote onboarding and launder stolen funds in Czechia [S1].

Evidence card B10 — 21 Aug 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

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

Note. Thread URLs are removed; illustrates why static PDF document uploads require independent verification.

Held

An August forum update expands a commercial document-forgery service to offer custom Czech proof-of-address, utility-bill, proof-of-income and payslip documents.

Not established

Successful bypass of any Czech lender, bank or identity-verification provider.

Evidence card B11 — 19 Aug 2026

Forum poster (alias withheld) | Forum thread | Forum | English

ORIGINAL

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

Note. Messenger IDs are removed; separate January and February threads also circulated Czech ID-and-selfie and 33-set passport archives.

Held

An August forum vendor lists EU identity-card front, back and selfie verification packs including Czechia at USD 25 each, alongside April forum recruitment paying USD 30 for live link-based EU KYC scans.

Not established

Authenticity of the identity documents, origin of the photos or successful financial onboarding.

Evidence card B12 — 12 Jan 2026

Forum poster (alias withheld) | Forum thread | Forum | Russian

ORIGINAL

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...

TRANSLATION

Registration of sole proprietors and companies to order in the CIS and Europe [...] Poland: sole proprietor USD 3,500, LLC USD 4,900. Czechia: sole proprietor USD 3,500, LLC USD 4,900. Standard package: bank account, electronic signature on hardware token, passport...

Note. A separate September forum post also marketed a multi-country mule and KYC worker network listing Czechia and Slovakia.

Held
A Russian-language forum vendor advertises turnkey nominee Czech sole-proprietor and limited-company registrations (USD 3,500 and USD 4,900) bundled with a bank account and hardware digital-signature token.

Not established
Actual Czech Trade Register filings, active shell companies or successful corporate bank onboarding.

Three commercial fraud layers recur in observed posts (`Case F`) [S1]:

- **Tailored domestic document forgery (`B10`).** On **21 August 2026**, a vendor advertised bespoke Czech proof-of-address utility bills, bank statements and employment payslips formatted to pass retail credit and account-opening checks [S1].
- **Low-cost EU KYC verification kits (`B11`).** On **19 August**, sellers offered **USD 25 EU KYC ID-and-selfie packs** explicitly covering Czechia [S1]. That complemented **19 April** recruitment paying **USD 30** for live verification links used to open payment and crypto accounts [S1].
- **Turnkey Czech corporate shells (`B12`).** On **12 January**, a vendor offered nominee **Czech sole proprietors (OSVČ) at USD 3,500** and **Czech limited-liability companies (s.r.o.) at USD 4,900** [S1]. The listing claimed delivery with business bank accounts and hardware digital-signature tokens [S1]. Combined with Czech eSIMs (`11 February`) and `SMS Arena` physical Czech SIM rentals (`21 November` , `Case E`), fraud rings assemble synthetic identities without visiting a branch [S1].

8.3 Payment-card material: a narrow observation

SCOPE OF THE CARD FIGURES

These figures describe a limited observed publication population. They do not estimate Czech card theft, national fraud losses or live payment validity.

Across observed Czechia-labelled underground posts between **1 January and 26 November 2026**, Brandefense counted **42 distinct Czechia-labelled payment card records** across **60 appearances in 55 posts**, spanning **21 distinct six-digit BINs** [S1]. By card network and labelled type, those 42 records split into **33 Mastercard** and **9 Visa**, and into **25 debit**, **4 credit**, **1 prepaid** and **12 unlabelled** cards [S1].

By publication venue (where one card may appear in multiple venues), **29** distinct cards appeared in automated checker-bot output, **14** in chat or channel posts and **1** on a forum [S1]. Checker status tags marked **11** approved or live, **8** network or processing error, **4** 3DS required, **5** declined and **20** unlabelled [S1].

Separately, **1,775 offer posts** referenced Czechia without clear-text card numbers, led by **1,570 multi-country card-shop updates** (median **51 countries** and **1,545 cards** per batch, asking **USD 10 to 25**) [S1]. Neither clear-text posts nor multi-country shop banners verify card validity, Czech issuer compromise or live balances [S1]. Card-fraud teams should act strictly on validated issuer BIN alerts and transaction telemetry rather than raw post counts [S1].

8.4 Secondary harm after legitimate Czech data breaches

Four confirmed commercial breaches (**Partners Group non-bank subsidiaries**, **BitFaktura**, **Rohlík.cz** and **Dedoles / `ui42`**) plus **Univerzita Karlova** show how stolen business context fuels follow-on fraud even when passwords and cards stay safe [S42][S44][S46][S52][S55]:

- **Invoicing and B2B redirection (`BitFaktura`).** Access to supplier directories, tax IDs and invoice histories enables convincing altered-IBAN payment emails aimed at Czech SME bookkeepers [S44][S45].
- **Order-context consumer smishing (`Rohlík.cz` and `Dedoles`).** Six months of Rohlík support transcripts and five years of Dedoles order records let scammers reference genuine deliveries, complaints or refunds by phone and SMS [S46][S47][S55][S56].
- **Advisory and university impersonation (`Partners Group` and `Charles University`).** Exposed financial-advisory client details and university student data support tailored investment scams, fake password-reset portals and fraudulent tuition or scholarship links [S43][S52][S54].

KEY TAKEAWAYS

01

Czech banking fraud hit CZK 11.8 billion attempted across 75,637 attacks in Q1–Q3 2026, while March police cases set a monthly record of 2,533.

02

ČTÚ anti-spoofing blocks shifted scammers from landline caller IDs into smishing, fake Portál občana logins and physical Czech SIM rentals.

03

Follow every Czech customer or invoicing breach immediately with clear anti-impersonation warnings and altered-IBAN payment checks.

CHAPTER 09

Banking, strong authentication and payment continuity

09

THIS CHAPTER ANSWERS

How are attackers targeting Bank iD, Czech retail clients and cash-out accounts?

10 of 25

selected Czech finance domains had a current credential listing on 27 November 2026

9.1 Selected finance-sector posture and licensed-bank exposure 69

9.2 Bank iD and MojeID demand, fake Portál občana lures and bank-mule brokers 70

9.3 DORA supervision, SDAT reporting and operational resilience 72

CHAPTER 09

Banking, strong authentication and payment continuity

IN SHORT

Czechia's banking perimeter is strongly hardened on mail hygiene: 23 of 25 finance domains (and 13 of 14 licensed commercial banks) enforce DMARC and 20 sign DNSSEC. Yet external exposure shows 10 of 25 finance domains (7 of 14 licensed banks) with current credential listings. Across 13 banks, 29,729 non-employee device associations most plausibly reflect infected customer devices, alongside Bank iD phishing and Telegram mule networks. Validate current listings first, separate employee from customer triage and automate ČNB's January 2027 DORA JSON switch.

9.1 Selected finance-sector posture and licensed-bank exposure

Across the **25-domain Banking and finance cell** (27 November 2026 snapshot, all 25 domains assessed), perimeter hygiene is Czechia's strongest while external exposure highlights customer-endpoint risk [S3][S4][S31]. Within the full 25-domain cell, **23 of 25 (92%)** enforce DMARC (**10** `reject`, **13** `quarantine`, **2** `none`, **0 missing**), **25** publish SPF, **20** expose DKIM, **20** publish DNSSEC DS and **21** enforce HSTS [S3]. On Brandefense Atlas exposure signals, **10 of 25** finance domains showed a current credential listing [S4]. Twenty-two finance domains had **at least 39,079 device associations** (**299 employee** across 16 domains; **38,780 non-employee**), and **24** had **204,055 historical credential records** [S4].

Narrowing strictly to the **14 licensed commercial banks** inside that cell clarifies where customer-device risk concentrates (preserving the smaller 14-bank denominator) [S3][S4]:

Metric (27 November 2026 snapshot)	Full finance cell (n = 25)	Licensed commercial banks (n = 14)	Operational takeaway	Sources
DMARC `reject` / `quarantine`	23 (10 reject, 13 quarantine)	13 (5 reject, 8 quarantine)	Strongest anti-spoofing baseline across all ten Czech sectors	[S3]
DMARC `none` / missing	2 none, 0 missing	1 none, 0 missing	Move any remaining monitoring-only bank domains to quarantine or reject	[S3]
SPF / DKIM / DNSSEC DS	25 / 20 / 20	14 / 10 / 12	Broad cryptographic DNS and mail-signing adoption	[S3]
Domains with current credential listing	10 domains	7 domains	Validate active listings within five working days	[S4]

Metric (27 November 2026 snapshot)	Full finance cell (n = 25)	Licensed commercial banks (n = 14)	Operational takeaway	Sources
Non-employee device associations	38,780 (22 domains)	29,729 (13 domains; top 3 hold 56.3%)	Primarily customer endpoints infected by infostealers, not bank servers	[S4]
Employee device associations	299 (16 domains)	200 (9 domains)	Reconcile against managed staff endpoints and revoke sessions	[S4]
Historical credential records	204,055 (24 domains)	Not published	Multi-year cumulative exposure; never equals a 2026 breach	[S4]
365-day domain mentions (chat / web)	2 domains (3) / 0	1 domain (2) / 0	Direct domain chatter stays minimal despite heavy Telegram mule volume	[S4]

Non-employee device counts (**29,729** across 13 licensed banks, with the top three banks holding **56.3%**) most plausibly reflect infected retail customer devices rather than intrusions into bank infrastructure [S4]. Clear-text card posts in §8.3 establish no validated card-to-bank relationship or issuer ranking [S1].

9.2 Bank iD and MojeID demand, fake Portál občana lures and bank-mule brokers

While bank domains stay quiet, Czech retail bank names and strong electronic identities sit at the centre of Czechia's underground fraud economy (`Case G`) [S1][S25][S31][S32].

Evidence card B15 — 12 Aug 2026

Channel poster (alias withheld) | Telegram channel | Telegram | Russian

ORIGINAL

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

TRANSLATION

Help me pass verification in the [Czech consumer app]. For verification, a Czech Bank iD is needed. USD 100 for each account, I need many.

Note. Guarantor-bot handles and app names are removed; directly parallels Bank iD and Portál občana official fraud warnings.

Held
An August Russian-language Telegram buyer explicitly offers USD 100 per account for bulk Czech Bank iD identity verifications, alongside separate August demand for Czech MojeID KYC ('WTB. KYC MojeID. Only Czech Republic') and February Bank iD account demand.

Not established
Completed Bank iD or MojeID fraud, bank compromise or participation by any Czech resident.

Evidence card B16 — 15 Jan 2026

Channel poster (alias withheld) | Telegram channel | Telegram | Russian

ORIGINAL

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.

TRANSLATION

Slovakia: all banks, handover in Bratislava. Czechia: [Czech retail banks], handover in Prague or remote. Poland: [Polish banks], Warsaw, Wrocław meeting/handover. Good percentage, clarify in PM.

Note. Bank names and handles are removed.

Held
A Russian-language Telegram broker advertises cross-border bank-account mule handovers across Prague, Bratislava, Warsaw and Wrocław, alongside January-October posts pricing Czech retail bank accounts at USD 170 to 700 or 20% to 35% cash-out commissions.

Not established
Compromise of any bank's systems, active mule headcount or verified transaction volume.

Two interlocking criminal markets drove Czechia's August–October Telegram spike [S1]:

- **Direct buyer demand for Czech electronic identity (B15).** Between **10 and 12 August 2026**, Telegram buyers advertised **USD 100 per Czech Bank iD account**, following 4 February betting-account demand [S1]. Another post sought `WTB. KYC MojeID. Only Czech Republic` [S1]. Official warnings from **Bank iD** (updated 9 November) and **Portál veřejné správy** describe SMS tax-refund and benefit lures leading to counterfeit Portál občana pages [S31][S32]. Those phishing sites capture Bank iD credentials and trick victims into forwarding confirmation codes or sending funds to "safe accounts" (bezpečný účet) [S31][S32]. Neither buyer demand nor phishing establishes any breach of Bank iD or MojeID infrastructure [S31].
- **Industrialised Central European bank-mule brokerage (B16).** Across 2026, Russian- and Ukrainian-language Telegram groups generated **28,287 financial-account buying or renting posts**, peaking at **13,457 in October** alone [S1]. Brokers recruited Czech retail accounts (known to Czech Police as **legalizační účty**) with handovers in **Prague, Bratislava, Warsaw and Wrocław** [S1][S25]. Ads quoted **USD 170 to 700 per account** or **20% to 35% cash-out commission** (specific bank names redacted) [S1]. High-speed instant CZK payments through ČNB's **CERTIS** rail give fraud teams only minutes to halt mule disbursements once a customer approves a social-engineered transfer [S27][S29].

9.3 DORA supervision, SDAT reporting and operational resilience

Under the EU Digital Operational Resilience Act (**DORA**, Regulation `EU 2022/2554`), the **Czech National Bank (ČNB)** supervises ICT risk, third-party oversight and major ICT incident reporting across Czech finance [S27][S28]. That mandate covers banks, insurers, payment institutions and market infrastructure [S27]. ČNB conducted its **first on-site DORA inspections in 2025** [S86]. Its annual supervisory review noted that common deficiencies stemmed less from novel rules than from gaps in internal processes, documentation and control execution [S86].

Under Commission Delegated Regulation `(EU) 2025/301` Article 5, financial entities submit major ICT incident reports to ČNB via the **SDAT** portal (`DORAEU01` / `DORAEU02`) [S28][S68]. Deadlines are **4 hours from classification** (no later than **24 hours from detection**) for initial notices, **72 hours** for intermediate reports and **1 month** for final reports [S68]. Crucially for 2026–2027 engineering roadmaps, ČNB's SDAT methodology confirms that structured **JSON reporting replaces Excel templates from 1 January 2027** [S28]. Banks should automate JSON incident-report generation well ahead of year-end and keep core banking networks strictly isolated from non-bank group subsidiaries and outsourced marketing or support vendors [S28][S42].

Partners Banka's August 2026 disclosure illustrates this architectural boundary in practice [S42]. When a cyberattack hit four affiliated non-bank Partners Group subsidiaries (`Case L`), the regulated bank's separated core environment remained unaffected [S42][S43].

KEY TAKEAWAYS

01

23 of 25 selected finance domains and 13 of 14 licensed Czech banks enforce DMARC with minimal domain mentions underground, pushing criminals toward client phishing and mule recruitment.

02

Explicit Telegram demand for Bank iD (USD 100) and MojeID plus Prague/Bratislava/Warsaw mule brokers (USD 170–700) connects directly to Czechia's CZK 11.8B fraud wave.

03

Pair mule-account AML detection and Bank iD anti-impersonation controls with automated JSON readiness for ČNB's January 2027 DORA SDAT cutover.

CHAPTER 10

Regulation, reporting duties and governance

THIS CHAPTER ANSWERS

Which Czech authority, portal, trigger and legal deadline apply after an incident?

24h / 72h / 30d

statutory Act No. 264/2025 Coll. incident-reporting sequence

10.1 Czechia's 2026 statutory map: Act No. 264/2025 Coll. and dual CSIRT routing 74

10.2 Multi-authority reporting matrix for Czech organisations 74

CHAPTER 10

Regulation, reporting duties and governance

IN SHORT

Cybersecurity Act No. 264/2025 Coll. (transposing NIS2) took effect on 1 November 2025. Under a 24 November 2026 contract, incident handling splits between NÚKIB (`GovCERT.CZ`) for higher-tier entities and CZ.NIC's `CSIRT.CZ` for lower-tier entities. Financial firms report to ČNB under DORA (`lex specialis`), personal-data breaches go to ÚOOÚ within 72 hours, and EU CRA Article 14 manufacturer reporting took effect on 11 September 2026. Verify portal access and reporting clocks today.

10.1 Czechia's 2026 statutory map: Act No. 264/2025 Coll. and dual CSIRT routing

Act No. 264/2025 Coll., on Cybersecurity (zákon o kybernetické bezpečnosti), entered into force on **1 November 2025**, replacing Act No. 181/2014 Coll. and transposing the EU NIS2 Directive into Czech law [S21]. Under **Section 6(1)**, organisations meeting regulated-service criteria must notify their regulated service to NÚKIB via **Portál NÚKIB** within **60 days** of meeting the conditions [S21]. Under **Section 15(1)–(2)**, Czech law establishes a two-tier incident-reporting architecture [S21][S24]:

- **Higher-obligation regime (režim vyšších povinností).** Entities report incidents directly to **NÚKIB (`GovCERT.CZ`)** [S21][S24].
- **Lower-obligation regime (režim nižších povinností).** Entities report incidents to the **National CERT (`CSIRT.CZ`)**, operated by association **CZ.NIC** under the renewed public-law contract signed with NÚKIB on **24 November 2026** [S21][S24].

Under **Section 15(4)**, newly registered entities receive a **one-year implementation period** from delivery of NÚKIB's registration decision before mandatory duties apply in full [S21]. Entities already regulated under legacy Act No. 181/2014 Coll. remain continuously bound under **Section 71(1)** [S21]. Under **Section 16(1) and (3)**, regulated entities submit an **early warning within 24 hours** and an **incident notification within 72 hours** (or **24 hours** for trust-service providers) [S21]. Progress updates follow on request, and a **final report is due within 30 days** [S21].

Maximum administrative fines under **Section 59(4)** and **Section 60(7)** reach **CZK 250 million or 2% of net worldwide annual turnover** (whichever is higher) for higher-obligation, strategic-service or notification-failure offences [S21]. Fines reach **CZK 175 million or 1.4%** for lower-obligation breaches and **CZK 100 million** for selected procedural offences [S21]. Under **Section 70**, EU sectoral cybersecurity rules such as **DORA** apply as lex specialis for financial entities to prevent duplicative ICT incident reporting [S21][S27].

10.2 Multi-authority reporting matrix for Czech organisations

Because a single ransomware attack or SaaS breach can trigger cybersecurity, financial, privacy and product-security clocks simultaneously, Czech legal and CISO teams should verify all five regimes below (operational guidance only, not legal advice):

Regime and Czech / EU statute	Competent authority & portal	Trigger	Statutory deadlines	Maximum penalty / statutory note	Sources
Cybersecurity Act (NIS2) (`Act No. 264/2025 Coll.` , Sections 6, 15, 16, 59, 60)	**NÚKIB** (`Gov-CERT.CZ` , Portál NÚKIB) for higher tier; **CSIRT.CZ** (`CZ.NIC`) for lower tier	Significant cyber incident affecting regulated service	**24h** early warning; **72h** notification (**24h** trust providers); **30 days** final report	Up to **CZK 250M / 2%** (higher) or **CZK 175M / 1.4%** (lower); 1-year ramp under Section 15(4)	[S21][S24]
Financial resilience (DORA) (`EU 2022/2554` , Del. Reg. `2025/301` Art. 5)	**ČNB** via **SDAT** (`DORAEU01` / `DORAEU02`)	Major ICT-related incident at supervised financial entity	**4h** from classification (max **24h** from detection); **72h** intermediate; **1 month** final	Lex specialis under Act 264/2025 Section 70; **JSON replaces Excel from 1 Jan 2027**; inspections active	[S21][S27][S28] [S68][S86]
Personal data protection (`GDPR` + `Act No. 110/2019 Coll.` , Section 62(5))	**ÚOOÚ** (Úřad pro ochranu osobních údajů)	Personal-data breach posing risk to individuals' rights	**72 hours** from becoming aware; without undue delay to affected people if high risk	GDPR fines apply to private controllers; **Section 62(5) waives administrative GDPR fines for public authorities** (distinct from Section 63 non-GDPR regime)	[S22][S33]
Product security (EU CRA) (`Reg. (EU) 2024/2847` , Arts. 14 & 71)	Designated CSIRT & ENISA Single Reporting Platform	Actively exploited vulnerability or severe incident in products with digital elements	**24h** early warning; **72h** notification; **14 days** (vuln) or **1 month** (incident) final	**Article 14 reporting applies from 11 September 2026**; general CRA obligations apply from **11 December 2027**	[S69]
Telecom & criminal reporting (Electronic Communications Act; Criminal Code Sections 230–232)	**ČTÚ** (telecom anti-spoofing); **Police ČR / NCOZ** (criminal offences)	Spoofed-call filtering / telecom incidents; extortion, fraud or intrusion	Operator anti-spoofing ongoing; criminal filing immediately on ransom or fraud	Preserves forensic chain of custody; supports international disruption (e.g. Operation Eastwood)	[S25][S34][S35] [S85]

Two Czech specifics deserve explicit board attention. First, **Act No. 110/2019 Coll. Section 62(5)** waives administrative GDPR fines for Czech **public authorities and public bodies** under GDPR Article 83(7) [S22]. However, public bodies that suffer a breach can still face mandatory ÚOOÚ notices, corrective orders, NÚKIB or CSIRT reporting, police investigations and heavy recovery costs [S22][S33].

Second, **Czech software, IoT and industrial-equipment manufacturers** entered live **EU Cyber Resilience Act Article 14** vulnerability-reporting obligations on **11 September 2026** [S69]. Manufacturers must file 24-hour early warnings for actively exploited flaws more than a year before full CRA conformity rules take effect on **11 December 2027** [S69].

KEY TAKEAWAYS

01

Act No. 264/2025 Coll. splits Czech NIS2 incident handling between NÚKIB (higher tier) and CZ.NIC's CSIRT.CZ (lower tier, confirmed by contract on 24 November 2026).

02

Financial institutions follow DORA [redacted] via ČNB's SDAT portal (moving to JSON on 1 January 2027), while Czech manufacturers entered CRA Article 14 reporting on 11 September 2026.

03

Pre-verify portal logins, delegated backups and separate awareness-versus-classification logs before an incident starts the 4-hour or 24-hour clock.

CHAPTER 11

Outlook and conditional triggers for 2027

11

THIS CHAPTER ANSWERS

Which observable triggers should shift Czech defensive posture into 2027?

5

conditional scenarios tied to measurable operational indicators

CHAPTER 11

Outlook and conditional triggers for 2027

IN SHORT

Rather than relying on generic forecasts, Czech defenders should tie 2027 posture shifts to five verifiable triggers. Watch Act No. 264/2025 Coll. grace-period completions, rapid PHP and CMS zero-day waves, Telegram bank-mule spikes, municipal and mid-market ransomware, and internet-exposed OT controllers. Pair each trigger with named telemetry so defensive escalation stays grounded in evidence.

Scenario	Observable trigger to monitor	Likely Czech operational impact	Pre-planned defensive shift	Sources
1. Act 264/2025 compliance wave completes	End of one-year grace periods (Section 15(4)) across newly registered entities plus live lower-tier onboarding into `CSIRT.CZ` and ČNB's 1 Jan 2027 SDAT JSON cutover	Higher reported incident baselines at NÚKIB and CSIRT.CZ; tighter supervisory audits on process and supplier documentation	Complete registration, test 24h/72h/30d and 4h DORA JSON templates and embed supplier breach SLAs into contracts	[S21][S24][S28][S86]
2. Sub-48-hour web-stack & edge zero-day waves	New CISA KEV or NÚKIB critical alerts on PHP, WordPress, Citrix NetScaler, Zimbra or widely deployed VPN/firewall gateways	Rapid opportunistic scanning and active exploitation (as seen in Aug `wp2shell` and Oct `PHP2Shell` at ČVUT)	Activate pre-authorised DMZ isolation playbooks, apply emergency patches within 48 hours and hunt pre-patch web shells	[S8][S15][S48][S49][S64][S79]
3. Mule-account & Bank iD phishing escalation	Renewed surge above 10,000 monthly Czechia-tagged Telegram financial-account posts, new Bank iD / Portál občana smishing kits or spike in `legalizační účty` fraud	Higher retail and SME losses despite 81% bank stop rates; faster CZK instant-payment cash-out via Prague/cross-border mules	Tighten mule-onboarding anomaly rules, expand out-of-band high-value confirmations and publish joint anti-impersonation alerts	[S1][S25][S29][S31][S32]

Scenario	Observable trigger to monitor	Likely Czech operational impact	Pre-planned defensive shift	Sources
4. Municipal & multi-branch ransomware persistence	Continued regional activity from the claimant labels listed in §7.1 against local offices, multi-branch retailers and mid-market supply chains	Multi-week cash-only or paper-and-pencil disruption at under-resourced towns and retail networks	Audit air-gapped or tape backup restores quarterly, segment municipal-police and branch networks and close local DMARC gaps	[S2][S3][S37][S39][S41][S57]
5. Internet-exposed OT & CRA reporting overlap	First confirmed Czech retail refrigeration or building-automation intrusion matching European cooling attacks, or active flaw in Czech-made connected hardware	Physical refrigeration spoilage, heating interruption or mandatory 24-hour CRA Article 14 manufacturer notifications	Remove every exposed cooling, HVAC and PLC controller from public IP space and test CRA Article 14 vulnerability intake	[S51][S58][S69]

KEY TAKEAWAYS

01

Treat Act 264/2025 grace-period expiry and ČNB's 1 January 2027 DORA JSON switch as hard engineering deadlines, not paper milestones.

02

Pre-authorise emergency web-stack isolation so future PHP or CMS waves never force ad-hoc decisions under fire.

03

Watch Telegram bank-mule spikes, exposed OT inventories and offline-backup restore tests as your primary early-warning indicators into 2027.

CHAPTER 12

Defender action plan and remediation reference

12

THIS CHAPTER ANSWERS

Who acts first, on what timeline and with what completion evidence?

0–90 days

sequenced defender roadmap plus verified CVE fixed-release table

12.1 Priority action lanes and completion evidence 81

12.2 Vulnerability remediation reference 83

12.3 Supporting continuous validation 84

CHAPTER 12

Defender action plan and remediation reference

IN SHORT

Patching critical PHP, WordPress, Citrix, Office, Zimbra and router flaws, isolating exposed OT controllers and validating offline backups start immediately rather than waiting for annual audit cycles. Assign each lane below to a named technical owner and business sponsor, and require dated verification evidence rather than policy documents to mark tasks complete.

12.1 Priority action lanes and completion evidence

1**Immediate (0–7 days)**

Inventory all public-facing PHP portals, WordPress sites, Citrix NetScaler gateways, Zimbra servers, exposed VNC hosts, legacy TP-Link/SOHO routers and refrigeration/HVAC controllers; apply current fixed builds in §12.2 (or replace End-of-Life hardware), remove OT and VNC from public IP space and pre-authorise emergency DMZ cut-offs

OWNER

Infrastructure, web ops, OT engineering and CISO

COMPLETION EVIDENCE

Signed external-asset register, patch/build logs, zero exposed VNC/OT scan and approved isolation runbook

Eliminate direct internet-facing RDP (`Case C`), enforce phishing-resistant MFA on VPN, webmail, Microsoft 365 and university/corporate SSO, block unnecessary Device Code Flow, restrict script execution against ClickFix lures and validate any current credential listing within five working days

OWNER

Identity and SOC leads

COMPLETION EVIDENCE

Firewall/RDP audit, Conditional Access export, dated listing dispositions and endpoint policy log

2**30 days**

Reconcile employee-labelled device associations (`24,224` across `168` domains) against managed corporate endpoints, revoke exposed sessions and route non-employee device signals (`294,482`) to customer-fraud controls

OWNER

Endpoint, identity and fraud leads

COMPLETION EVIDENCE

Reconciled device-triage register with dated revocations or documented closure

Close the 71 non-enforcing DMARC domains (prioritising regional/local administration, manufacturing and transport), verify SPF/DKIM alignment, remediate invalid TLS certificates and enable HSTS and CAA on public portals

OWNER

Messaging security and domain owner

COMPLETION EVIDENCE

Live DNS DMARC (`quarantine` / `reject`), TLS and HSTS check across all owned domains

Verify Act No. 264/2025 Coll. registration status on Portál NÚKIB, test higher-tier (`GovCERT.CZ`) or lower-tier (`CSIRT.CZ`) reporting paths, validate ÚOOÚ 72-hour workflows and test CRA Article 14 intake (for product makers); financial entities verify ČNB SDAT JSON automation ahead of 1 January 2027

OWNER

Legal, compliance and CISO

COMPLETION EVIDENCE

Dated portal login check, delegated backup roster, JSON test output and incident-clock playbook

3**60 days**

Audit all IT supplier credentials (`ui42` lesson), revoke dormant vendor access, purge retired e-commerce or support archives (`Dedoles` and `Rohlík.cz` lessons), enforce least-privilege access between web apps and central databases (`Charles University` lesson) and verify strict separation between banks and non-bank subsidiaries (`Partners Banka` lesson)

OWNER

Vendor risk, application security and DPO

COMPLETION EVIDENCE

Revocation log, archive-deletion certificate, DB-privilege audit and network-segmentation diagram

For retail banks, payment providers and e-commerce operators, tighten AML mule-account onboarding checks against forged Czech payslips and nominee shells, tune Bank iD / Portál občana anti-impersonation alerts and brief SME finance teams against altered-IBAN invoice fraud (`BitFaktura` lesson)

OWNER

Fraud operations, AML and digital channels

COMPLETION EVIDENCE

Updated AML rule-test report, customer warning templates and finance callback verification log

4**90 days**

Run a full offline-backup restoration and manual-fallback exercise (paper-and-pencil branch or cash-only municipal continuity, following Náměšť nad Oslavou, Židlochovice and PRO-DOMA) plus a crisis-communications drill separating cyber intrusions from technical outages and hacktivist claims

OWNER

Executive sponsor, continuity lead and CISO

COMPLETION EVIDENCE

Dated restore-time log, offline-fallback drill notes and approved crisis-messaging templates

12.2 Vulnerability remediation reference

The table below compiles affected and fixed versions from archived NVD, CVE CNA and vendor records for the critical vulnerabilities referenced in this report. Historical earlier fixes do not substitute for later cumulative releases on supported branches:

Product and CVEs	Affected versions	Fixed versions and replacement guidance	Sources
PHP (`CVE-2026-109618` , `CVE-2026-109619` [PHP2Shell]; plus separate 19 Nov `CVE-2026-115560` / `GHSA-658j-r8rw-q6mx`)	For `CVE-2026-109618` / `109619` : PHP `8.5` before `8.5.12` , `8.4` before `8.4.27` , `8.3` before `8.3.36` , `8.2` before `8.2.35` and EOL `8.1` and older. For 19 Nov `CVE-2026-115560` : PHP `8.5` before `8.5.13` , `8.4` before `8.4.28` , `8.3` before `8.3.37` , `8.2` before `8.2.36` (including October fixes) and unsupported older branches.	Upgrade immediately to **19 November releases** `8.5.13` , `8.4.28` , `8.3.37` or `8.2.36` (or later supported releases / OS vendor LTS backports) [S64][S65]. Migrate EOL `8.1` and older (PHP `8.2` reaches EOL 31 December 2026). For `CVE-2026-115560` (session upload progress enabled plus mismatched `session.serialize_handler` across runtime or shared session stores), keep `session.upload_progress.enabled=0` in `php.ini` / FPM pool config with workers restarted and align serializers across shared stores [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` before `6.9.5` and `7.0.x` before `7.0.2` . `CVE-2026-60137` : WordPress `6.8.x` before `6.8.6` , `6.9.x` before `6.9.5` and `7.0.x` before `7.0.2` .	Upgrade immediately to WordPress `6.8.6+` , `6.9.5+` or `7.0.2+` (latest supported maintenance release) [S63][S77][S78]. Both CVEs are in CISA KEV; audit themes and plugins passing untrusted input to `WP_Query` `author__not_in` and inspect affected web roots for post-exploitation web shells and ClickFix scripts.	[S8][S15][S60][S63][S77][S78]

Product and CVEs	Affected versions	Fixed versions and replacement guidance	Sources
Citrix NetScaler ADC and Gateway (`CVE-2026-88771` , `CVE-2026-88772` ; superseded by 12 Nov `CTX697305` / `CVE-2026-120868`)	For Sep zero-days (`CVE-2026-88771` / `88772`): ADC/Gateway `14.1` before `14.1-73.37` , `13.1` before `13.1-64.23` , `14.1` FIPS before `14.1-73.37` FIPS, `13.1` FIPS/NDcPP before `13.1-37.279` . For 12 Nov `CTX697305` (`CVE-2026-120868`): supported `14.1` and `13.1` builds prior to Citrix's 12 November `CTX697305` cumulative security builds and EOL branches.	Apply Citrix's current **12 November** `CTX697305` supported builds (or later) across standard, FIPS and NDcPP appliances rather than stopping at September minima [S79][S80][S81]. Migrate EOL appliances, hunt for pre-patch persistence and rotate session secrets and keys.	[S79][S80][S81]
Microsoft Office (`CVE-2026-21509` , `Operation Neusploit`)	Unpatched Microsoft Office installations vulnerable to local security-feature bypass via untrusted inputs (published 26 Jan 2026; CISA KEV).	Apply Microsoft's January 2026 (and subsequent cumulative) Office security updates across all Windows endpoints and enforce Protected View and attack-surface reduction rules [S6][S18][S82].	[S6][S18][S82]
Zimbra Collaboration (ZCS) (`CVE-2025-66376`)	Zimbra Collaboration `10.0` before `10.0.18` and `10.1` before `10.1.13` (Classic UI stored XSS via CSS `@import` in HTML email; CISA KEV).	Upgrade to the latest supported `10.1.x` security release (minimum `10.1.13`) [S83]. Because ZCS `10.0` reached End of Life on 31 December 2025, migrate `10.0` and older Czech self-hosted mail servers to supported `10.1.x` builds.	[S8][S18][S83]
TP-Link SOHO routers (`CVE-2023-50224`)	Legacy End-of-Life TP-Link routers and access points including `TL-WR841N` (`dropbearpwd` improper authentication on `httpd` ; CISA KEV).	Replace unpatched End-of-Life SOHO routers with vendor-supported models receiving active security updates; where interim firmware exists per TP-Link FAQ 5058, patch immediately, disable WAN management and rotate default passwords [S61][S62][S84].	[S7][S61][S62][S84]

12.3 Supporting continuous validation

Organisations seeking tailored visibility into domain exposure, infostealer-credential alerts, lookalike domains and underground claims targeting Czech brands can request a Brandefense briefing at Brandefense demo request.

KEY TAKEAWAYS

01

Patch PHP, WordPress, Citrix NetScaler, Office, Zimbra and legacy routers immediately using §12.2 verified builds and remove exposed VNC and OT from public IP space.

02

Close the 71 non-enforcing DMARC domains and test Act 264/2025, CSIRT.CZ and ČNB SDAT JSON workflows within 30 days.

03

Require dated offline-backup restoration logs, vendor-revocation records and AML test reports to mark 60–90 day milestones complete.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Appendix A. Method, scope and exclusions · Appendix B. Evidence register · Appendix C. Sources · Appendix D. Glossary

86
sources

Appendix A. Method, scope and exclusions 87
Appendix B. Evidence register 89
Appendix C. Sources 90
Appendix D. Glossary 95

Appendix A. Method, scope and exclusions

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

A.1 Observation windows and evidence separation

Distinct reference dates apply across this report and are never combined into a single denominator. The primary 2026 activity window spans **1 January to 26 November 2026** (UTC, by publication timestamp) for underground posts (`53,404`), Ransompedia listings (`50`), 2026 domain mentions (`1,334`) and public incidents [S1][S2][S4]. Within that window, **12 to 26 November 2026** (`1,771` posts, `53` forum posts, `3` Ransompedia entries and `3` confirmed public incidents) is examined separately in §5.3 without extrapolating short-window figures to full-year rates [S1][S2].

Rolling 365-day dark-chat and dark-web domain mentions span **27 November 2025 to 26 November 2026** [S4]. Passive configuration checks (**250 domains**) reflect a **27 November 2026** snapshot, and all external official, statutory, NVD and press sources were verified on **27 November 2026** [S3].

A.2 Underground post population and corpus boundary

Observed Czechia-tagged posts total **53,404** across Telegram (`52,926`), forums (`428`), Discord (`25`) and paste sites (`25`) [S1]. August (`6,655`), September (`8,940`) and October (`18,965`) account for **34,560 posts (64.7%)** [S1]. That peak reflects Russian- and Ukrainian-language Telegram bank-drop and KYC brokerage chats (`13,457` financial-account posts in October alone) rather than intrusions into Czech bank infrastructure [S1]. November is partial through 26 November (`3,893` posts, including `101` forum posts, not all Czech-targeted) [S1]. Post cards `B01` through `B16` represent verbatim published excerpts and do not establish completed transactions or confirmed breaches on their own [S1].

A.3 Selected 250-domain portfolio, Atlas exposure and configuration snapshot

The Czech domain portfolio comprises **250 domains** in ten equal sector cells of 25, assessed on **27 November 2026** [S3][S4]. Selection is purposive rather than a statistical census of all Czech entities. Only the single national Atlas headline (**48/100**) is published; no per-sector, per-group or organisation exposure ratings appear anywhere in this report [S4].

Portfolio exposure signals comprise current credential listings (`66` domains, all 66 with history, `5,431` entries) and cumulative device associations (at least `318,706` , including `24,224` employee across `168` domains) [S4]. They also include historical credential records (`180,747,551` , with `99.4%` in Telecom), document associations (`1,010` across `101` domains) and 30-day similar-name observations (`68,245` across `201` domains) [S4]. These signals may overlap and never represent unique people, 2026-only activity or confirmed incidents [S4].

Published DMARC policy categories (`reject` , `quarantine` , `none` , missing) record DNS policy state rather than guaranteed `pct=100` enforcement or receiver handling under RFC 7489 [S70]. TLS (`8` of `250`) and HTTP (`23` of `250`) endpoints that could not be assessed are reported as separate counts [S3]. Separately, rolling 365-day

domain mentions (33 domains, 1,931 dark-chat; 16 domains, 230 dark-web) and 2026 subset mentions (23 domains, 1,334) cover all 250 domains [S4]. Licensed commercial-bank counts in §9.1 cover a strict **14-domain subset** inside the 25-domain Banking and finance cell [S3][S4].

A.4 Ransomware listings and payment-card scope

Ransompedia recorded **50 Czechia-labelled listings** across 20 claimant labels through 26 November 2026 (versus 27 in full-year 2025) [S2]. Two repeat entries leave at most 48 distinct claimed entities; five entries (covering four confirmed public Czech cases) match public reporting, while **45 remain unverified and strictly withheld** [S2].

SCOPE OF THE CARD FIGURES

Payment-card figures describe a limited observed publication population. They do not estimate Czech card theft, national fraud losses or live payment validity.

Observed posts contained **42 distinct Czechia-labelled card records** (60 appearances across 55 posts, 21 BINs) and **1,775 offer posts** without clear-text numbers (1,570 multi-country shop updates) [S1]. Neither count verifies issuance, stolen status or issuer compromise [S1].

A.5 Naming policy and explicit exclusions

Czech and cross-border organisations are named only where officially confirmed and widely reported in public Czech or international media (public_names.json). All personal names (officials, executives, spokespeople and affected individuals) are omitted. All 45 unconfirmed Ransompedia entries are withheld without pairing dates, sectors and labels, and all unconfirmed forum/Telegram targets and private portfolio domains are withheld. Four notable items were explicitly excluded from 2026 Czech cyber-incident counts:

1. **13 November 2026 ministry outage.** Affecting the ministries of Finance, Transport and Education the same day as the Charles University SIS breach; confirmed by Microsoft Czechia as a non-cyber internal technical failure [S54].
2. **Historical 2022–2024 APT31 MZV intrusion.** Attributed publicly in May 2025; cited strictly as pre-2026 baseline context from NÚKIB's 2025 Annual Report [S5].
3. **Unverified hacktivist camera and heating-control claims.** Telegram assertions by Z-Pentest Alliance and peers (January, May, October) lacked confirmation in independent Czech press and technical checks [S1][S58].
4. **August–October Telegram bank-mule brokerage surge.** Multi-country cash-out recruitment templates (34,560 posts in Aug–Oct) reflect retail fraud rails rather than Czech bank compromises [S1].

Appendix B. Evidence register

Verbatim excerpts are shown inline in the chapters listed below. Post dates reflect publication time; no card establishes a completed transaction or confirmed intrusion on its own.

Card	Date	Venue	Alias	Language	Section
B01	2026-02-18	Forum thread	Alias withheld	English	§4
B02	2026-02-24	Forum thread	Alias withheld	English	§4
B03	2026-01-29	Telegram channel	Alias withheld	Russian	§4
B04	2026-04-14	Forum thread	Alias withheld	English	§4
B05	2026-01-24	Forum thread	Alias withheld	English	§4
B06	2026-05-15	Forum thread	Alias withheld	English	§4
B07	2026-03-02	Forum thread	Alias withheld	English	§4
B08	2026-07-23	Forum thread	Alias withheld	English	§4
B09	2026-11-21	Forum thread	Alias withheld	Russian	§4
B10	2026-08-21	Forum thread	Alias withheld	English	§8
B11	2026-08-19	Forum thread	Alias withheld	English	§8
B12	2026-01-12	Forum thread	Alias withheld	Russian	§8
B13	2026-11-22	Forum thread	Alias withheld	English	§4
B14	2026-11-19	Forum thread	Alias withheld	English	§4
B15	2026-08-12	Telegram channel	Alias withheld	Russian	§9
B16	2026-01-15	Telegram channel	Alias withheld	Russian	§9

Appendix C. Sources

S1: Odin by Brandefense. Observed underground posts and publication counts (1 Jan-26 Nov 2026; recent 12-26 Nov 2026). Verified on 2026-11-27.

S2: Ransompedia. Country-labelled ransomware listings (1 Jan-26 Nov 2026 and full-year 2025). Verified on 2026-11-27.

S3: Odin by Brandefense. Configuration snapshot of 250 selected Czech domains (27 Nov 2026). Verified on 2026-11-27.

S4: Odin by Brandefense. Brandefense Atlas exposure observations across 250 assessed Czech domains (27 Nov 2026) and rolling 365-day domain mentions (27 Nov 2025 to 26 Nov 2026). Verified on 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 Verified on 2026-11-27.

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

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

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

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

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

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

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

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

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

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

Appendix D. Glossary

- **National Atlas headline.** The single 0 to 100 Brandefense Atlas exposure figure published for the assessed portfolio as a whole [S4]. Higher values indicate greater observed external exposure and never represent a breach percentage or sector ranking [S4].
- **Act No. 264/2025 Coll. (Zákon o kybernetické bezpečnosti).** Czechia's Cybersecurity Act transposing the EU NIS2 Directive, effective 1 November 2025, establishing higher- and lower-obligation tiers and 24h/72h/30d reporting clocks [S21].
- **Bank iD.** Czech bank-issued electronic identity scheme enabling citizens to authenticate to Portál občana, public services and commercial portals using retail banking credentials [S31].
- **BIN (bank identification number).** Leading six digits of a payment card number identifying the card network and issuing institution [S1].
- **CERTIS.** Czech National Bank's real-time interbank CZK payment clearing system [S27].
- **ClickFix.** Social-engineering technique prompting victims to copy and run malicious shell commands from fake verification or error prompts [S60].
- **CSIRT.CZ.** Czechia's National CSIRT operated by association CZ.NIC, designated for lower-obligation incident reporting under Act No. 264/2025 Coll. and a renewed 24 November 2026 public-law contract [S23][S24].
- **DMARC / SPF / DKIM.** Domain email-authentication standards declaring authorised sending hosts (SPF), cryptographic signatures (DKIM) and receiver handling policies for unaligned mail (DMARC) [S70][S71][S72].
- **DNSSEC.** Cryptographic signing extension for DNS records (evidenced by DS records in the parent zone) protecting domain lookups from spoofing [S3].
- **DORA / SDAT.** EU Digital Operational Resilience Act (`EU 2022/2554`) and the Czech National Bank's SDAT portal (`DORAEU01` / `DORAEU02`) for major financial ICT incident reporting [S27][S28][S68].
- **EU CRA (Cyber Resilience Act).** Regulation `(EU) 2024/2847` introducing mandatory 24-hour manufacturer reporting for actively exploited vulnerabilities in connected products from 11 September 2026 [S69].
- **HSTS.** HTTP Strict Transport Security header instructing browsers to connect strictly over encrypted HTTPS [S73].
- **KYC (Know Your Customer).** Identity-verification and customer due-diligence controls required before opening bank, payment or crypto accounts [S1].
- **Legalizační účty (money-mule accounts).** Retail bank accounts recruited, bought or rented by fraud brokers to receive and quickly forward stolen funds [S1][S25].
- **MojeID.** National digital-identity service operated by CZ.NIC supporting citizen access to Czech online public and commercial portals [S1].
- **NÚKIB (`GovCERT.CZ`).** Czechia's National Cyber and Information Security Agency (Národní úřad pro kybernetickou a informační bezpečnost), supervising higher-obligation entities and operating the Government CERT [S5][S21].

- **PHP2Shell / `wp2shell`.** Public labels for critical 2026 remote code execution vulnerability chains in PHP (`CVE-2026-109618`, `CVE-2026-109619`) and WordPress core (`CVE-2026-63030`, `CVE-2026-60137`) [S63][S74] [S75][S77][S78].
- **Portál občana.** Czechia's central online Citizen Portal linking residents to tax, registry and government e-services, frequently spoofed in Bank iD phishing [S32].
- **TLP:CLEAR.** Traffic Light Protocol label permitting unrestricted public sharing while observing privacy and legal duties.
- **ÚOOÚ.** Office for Personal Data Protection (Úřad pro ochranu osobních údajů), Czechia's GDPR supervisory authority [S22][S33].

About this report

Prepared by Odin by Brandefense. Version 1.0 applies distinct reference dates. The 2026 activity window runs from 1 January to 26 November 2026 (with 12 to 26 November examined separately), while rolling 365-day domain mentions span 27 November 2025 to 26 November 2026. Brandefense Atlas exposure assessments and passive configurations across all 250 selected domains reflect a 27 November 2026 snapshot. All public sources were verified on 27 November 2026.

The Czech edition translates the English master; the English edition prevails where wording differs. Recommendations require validation against each organisation's own assets, service dependencies and legal obligations.

© 2026 Brandefense. All rights reserved.

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