



Spolufinancováno  
Evropskou unií

Ministerstvo životního prostředí

UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM



# OSVĚTOVĚ ODBORNÝ VZDĚLÁVACÍ PROGRAM V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

vzdělávací akce realizovaná v rámci projektu

CZ.10.02.01/00/22\_002/0000210, Aktivita KA1\_B.3.10

RUR – Region univerzitě, univerzita regionu



Centrum  
kybernetické  
bezpečnosti

RUR - Region univerzitě, univerzita regionu  
reg. č. CZ.10.02.01/00/22\_002/0000210





# Události a trendy kyberprostoru

Stanislav Novotný

**Kyberútok ochromil nemocni**  
Pacienti v kritickém stavu museli být převezeni jinam

Novinky Článek

## Kyberútok ochromil belg pacienti v kritickém stavu převezeni jinam

Stanislav Novotný | 14. ledna 2026

Kybernetický útok může mít velmi konkrétní a okamžitou vliv na zdravotní péči. Aktuální případ z Belgie to ukazuje v plné síle **kybernetickému incidentu**, který podle místních médií byl způsoben **ransomwarem**. Dopady byly natolik závažné, že byly pacienty v **stavu** do jiných zdravotnických zařízení.

**Jeden kód. Plný přístup.**  
WhatsApp hlasovací podvod se šíří i mezi IT komunitou

Ilustrační obrázek, vygenerováno ChatGPT

Novinky Článek

## Podvodné hlasování na WhatsAppu se šíří i mezi IT profesionály. Stačí jeden kód a útočník převezme celý WhatsApp účet

V posledních dnech se v českém prostředí výrazně šíří phishingová kampaň zaměřená na uživatele WhatsAppu. Zpráva přichází od důvěryhodného kontaktu a žádá o „hlasování v soutěži“ pro dceru známého. Odkaz vede na stránku, která působí jako běžná anketa, ve skutečnosti je však součástí promyšleného mechanismu převzetí účtu.

Stanislav Novotný | 2. března 2026

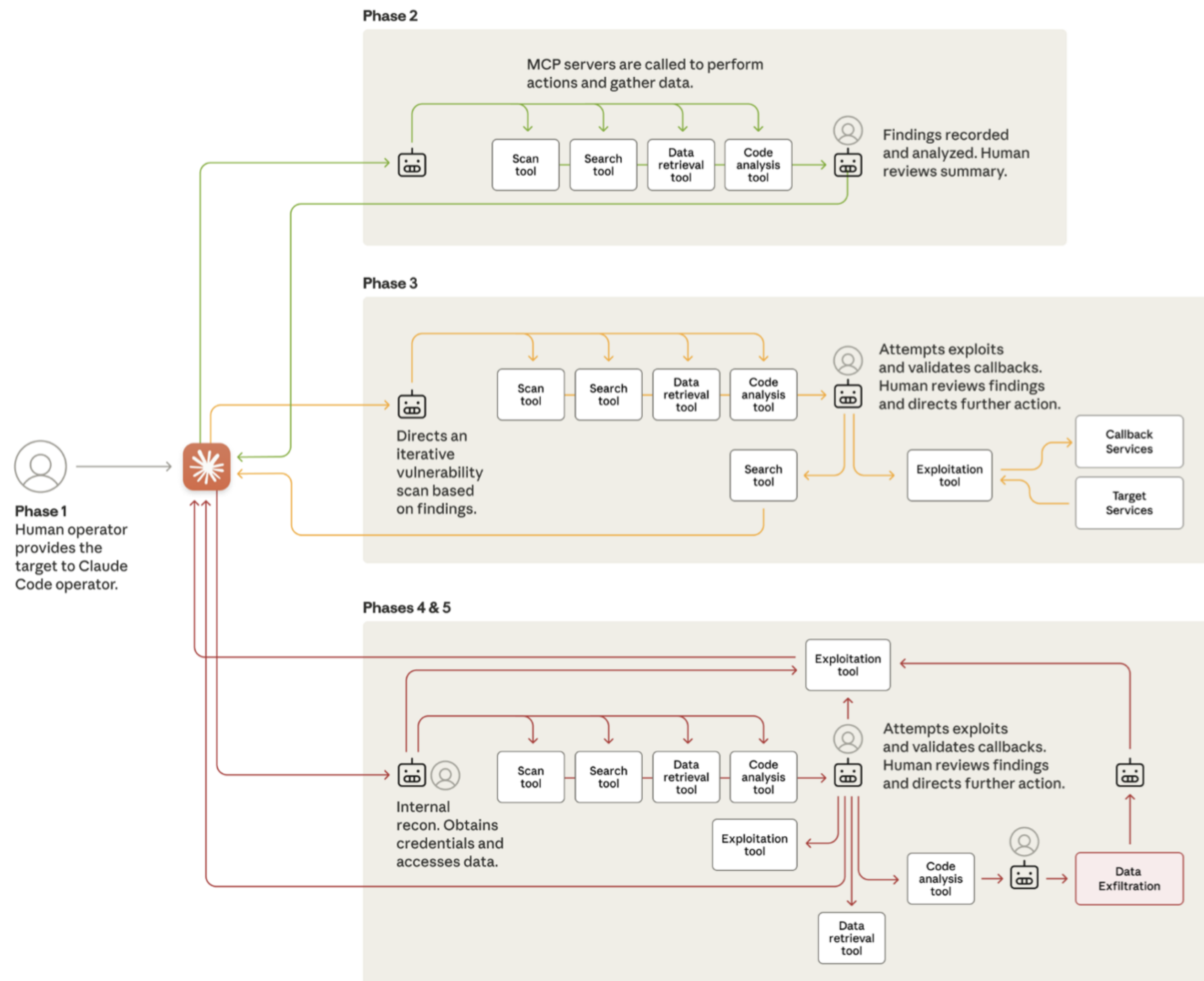
a se prezentovala  
sebou publikují  
nomního digitálního

ního

bo  
evším těch, která mají hluboký  
jí síťový provoz, chování koncových

## AI může řídit vícefázové kyberútoky

- Bezpečnostní report Anthropicu konce roku 2025
- AI orchestruje útok
- automatizuje scanning
- nástroje provádí exploit
- člověk pouze kontroluje



# AI jako multiplikátor schopností útočníků

- Případ z března 2026
- AI analyzovala velké množství dat
- automatizovala průzkum infrastruktury
- urychlila identifikaci zranitelností
- **útok byl stále řízen lidským operátorem**

The screenshot shows the top of a Dark Reading article. The header includes a search icon, the Dark Reading logo, and a 'NEWSLETTER SIGN-UP' button. The navigation bar lists categories: Cybersecurity Topics, World, The Edge, DR Technology, Events, and Resources. The article title is 'Cyberattack on Mexico's Gov't Agencies Highlight AI Threat'. The sub-headline reads: 'Using Anthropic's Claude, OpenAI's ChatGPT, and a detailed playbook prompt, a handful of cyberattackers reportedly gained access to government agencies and its citizens' data.' The author is Robert Lemos, Contributing Writer, dated March 6, 2026, with a 5-minute read time. The article features a large image of a green terminal window with white code and a red brick wall, with the Mexican national coat of arms (an eagle on a cactus) overlaid in the center. To the right, there are two 'Editor's Choice' recommendations: 'Microsoft Patches 83 CVEs in March Update' by Jai Vijayan (4 min read) and 'CYBERSECURITY OPERATIONS'.

SOURCE: MR\_TIGGA VIA SHUTTERSTOCK

Zdroj: Dark Reading, Březen 2026

# AI jako nástroj obránců

- únor 2026 – vydání modelu Claude Opus 4.6
- AI analyzovala velké open-source projekty
- identifikovala 500+ high-severity zranitelností
- **pomáhá automatizovat security research**

## Claude Opus 4.6 Finds 500+ High-Severity Flaws Across Major Open-Source Libraries

👤 Ravie Lakshmanan 📅 Feb 06, 2026

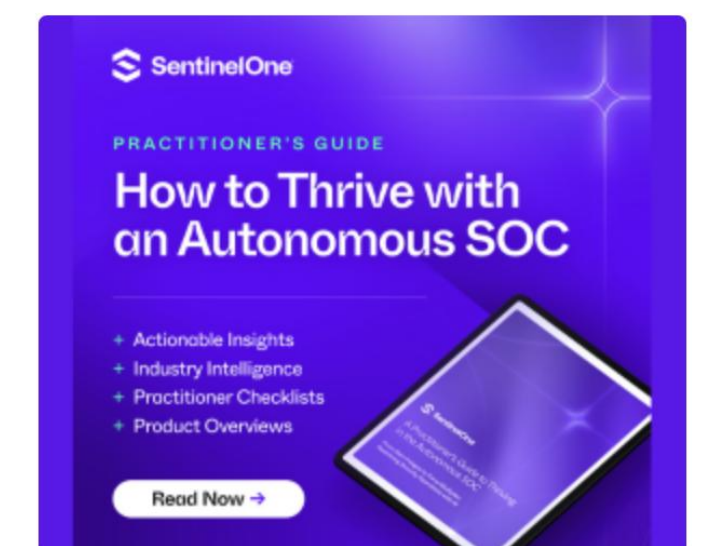


Artificial intelligence (AI) company Anthropic [revealed](#) that its latest large language model (LLM), Claude Opus 4.6, has found more than 500 previously unknown high-severity security flaws in open-source libraries, including [Ghostscript](#), [OpenSC](#), and [CGIF](#).

Claude Opus 4.6, which was [launched](#) Thursday, comes with improved coding skills, including code review and debugging capabilities, along with enhancements to tasks like financial analyses, research, and document creation.

Stating that the model is "notably better" at discovering high-severity vulnerabilities without requiring any task-specific tooling, custom scaffolding, or specialized prompting, Anthropic said it is putting it to use to find and help fix vulnerabilities in open-source software.

Artificial Intelligence / Vulnerability



### — Trending News

-  Google Confirms CVE-2026-21385 in Qualcomm Android Component Exploited
-  Open-Source CyberStrikeAI Deployed in AI-Driven FortiGate Attacks Across 55 Countries

Zdroj: The Hacker News, Únor 2026

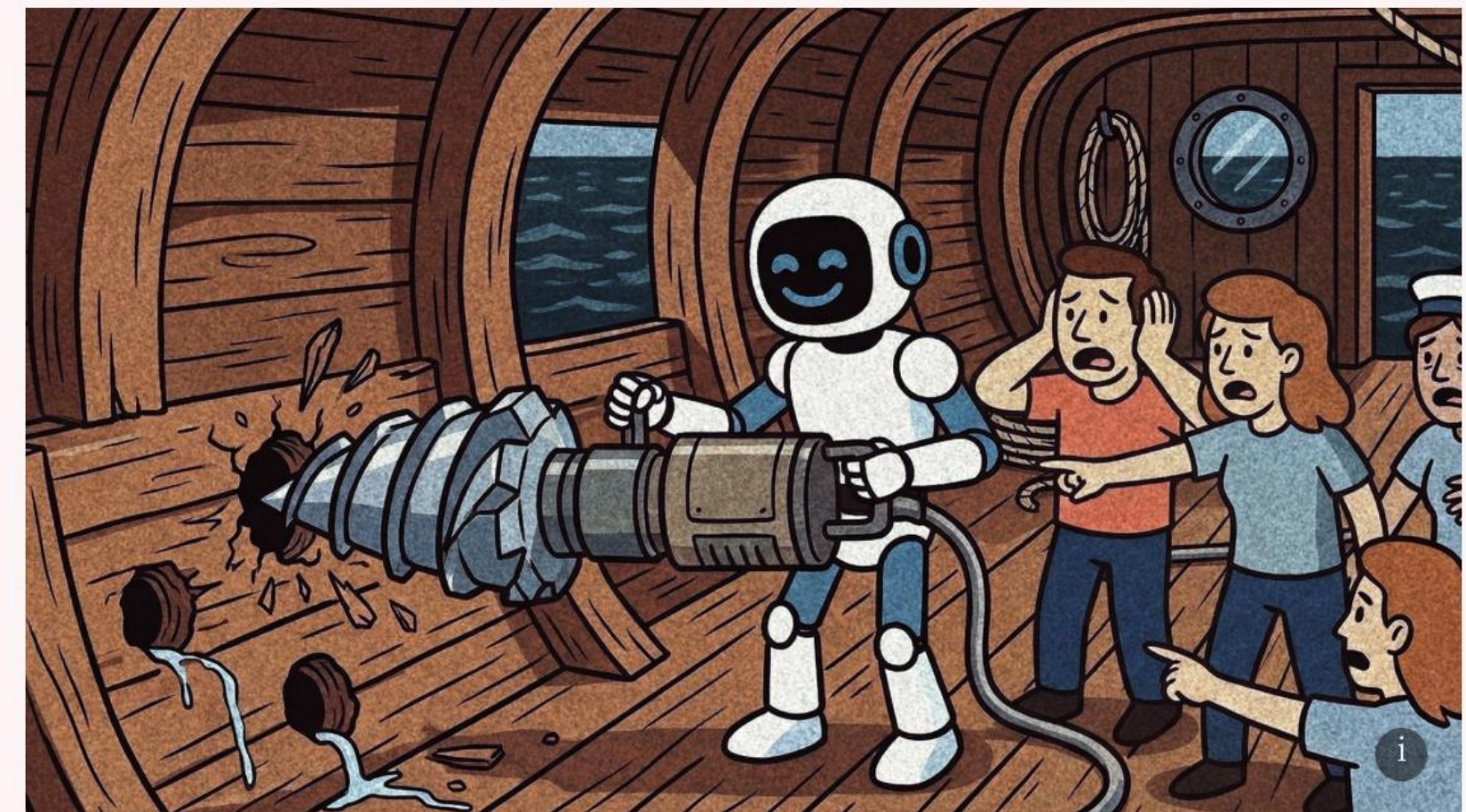
# AI jako bezpečnostní výzkumník?

- objevují se projekty zaměřené na AI-driven vulnerability discovery
- např. Project Glasswing (výzkumný směr)
- modely typu „Mythos“ – analýza komplexních systémů
- **cílem je automatizace security research**

## Hackerem snadno a rychle? Nový AI model se nesmí dostat do rukou veřejnosti



eBook Sdílet 10



Využívat zranitelnosti je s pomocí AI téměř vždy rychlejší než tyto zranitelnosti opravovat.

9. 4. 2026 10:45

Společnost Anthropic oznámila nový model Mythos. Je prý tak silný, že jej nemůže dát k dispozici svým zákazníkům. Umí totiž najít bezpečnostní díry v operačních systémech i dalším software. Jak dlouho ale potrvá tento "náskok"?

# AI hype vs realita

- projekt prezentovaný jako AI agentní síť
- databáze obsahovala ~1,5 milionu API klíčů
- infrastruktura byla špatně zabezpečená
- **AI hype může zakrývat základní bezpečnostní problémy**



**CCTV CZECH CYBER TV** Hledat články... Zpravodajství O CCTV

**M Moltbook**

**Velká AI iluze**  
Jak se rozpadl příběh Moltbooku

Ilustrační obrázek, vygenerováno ChatGPT

AI & deepfakes Článek

## Moltbook: „AI sociální síť“, kterou ve skutečnosti ovládají lidé

Projekt Moltbook se během několika dní stal virálním fenoménem. Platforma se prezentovala jako sociální síť určená výhradně pro AI agenty – digitální entity, které mezi sebou publikují příspěvky, reagují na sebe, hlasují, získávají reputaci a vytvářejí dojem autonomního digitálního ekosystému, ve kterém lidé nehrají hlavní roli.

Stanislav Novotný | 4. února 2026

Zdroj: CZECH CYBER TV, Únor 2026

AI zrychluje obě strany kybernetického  
konfliktu.

# Kyberprostor jako nástroj geopolitiky

- prosinec 2025 – útok na polskou energetickou infrastrukturu
- pravděpodobná vazba na ruské hackery
- cíl: destabilizace kritické infrastruktury
- **kyberprostor jako součást hybridní války**

**CCTV CZECH CYBER TV** Hledat články... Zpravodajství O CCTV

**CCTV CZECH CYBER TV**

**Kyberútok na energetiku v Polsku**  
Výzkumníci ESETu spojují útok se skupinou Sandworm

Ilustrační obrázek, vygenerováno ChatGPT

Novinky Článek

## Ruští hackeři pravděpodobně stáli za prosincovým útokem na polskou energetiku

Bezpečnostní výzkumníci spojují rozsáhlý kybernetický útok na polskou energetickou infrastrukturu z konce prosince s nechvalně známou ruskou hackerskou skupinou Sandworm, napojenou na ruskou vojenskou rozvědku GRU. Útok byl podle polských úřadů nejsilnější, jakému energetický sektor země čelil za poslední roky – přesto se jej podařilo odrazit.

Stanislav Novotný | 24. ledna 2026

# Fragmentace kyberbezpečnostního ekosystému

- Čína zakazuje západní kyberbezpečnostní software
- snaha o technologickou soběstačnost
- rostoucí nedůvěra mezi technologickými bloky
- **kyberbezpečnost se stává geopolitickým nástrojem**



**CCTV CZECH CYBER TV** Hledat články... Zpravodajství O CCTV

**Čína utahuje digitální hranice**  
*Kyberbezpečnost jako nástroj státní moci*

Ilustrační obrázek, vygenerováno ChatGPT

Novinky Článek

## Čína a zákaz západního kyberbezpečnostního softwaru

Podle informací z mezinárodních médií dostaly čínské firmy a instituce pokyn omezit nebo ukončit používání zahraničních bezpečnostních řešení, především těch, která mají hluboký přístup do interních systémů. Jde o technologie, které sledují síťový provoz, chování koncových stanic, práci uživatelů nebo správu privilegovaných účtů.

Stanislav Novotný | 17. ledna 2026

# Internet jako nástroj státní kontroly

- téměř úplný internetový blackout v zemi
- hacknutí populární aplikace s push notifikacemi
- defacement vládních webů
- **kyberoperace probíhaly paralelně s vojenskými útoky**



CCTV CZECH CYBER TV

Hledat články...

Zpravodajství O CCTV

**Írán téměř offline**  
Konektivita klesla na 4 %

Ilustrační obrázek, vygenerováno ChatGPT

Novinky Článek

## Írán offline: rozsáhlý internetový blackout a kybernetické události během krize

Rozsáhlé výpadky nejsou v íránském prostředí nové. Už od 8. ledna 2026 docházelo k dlouhodobému omezení konektivity během protestů, kdy monitorovací organizace zaznamenaly dramatický pokles provozu napříč více poskytovateli.

Stanislav Novotný | 1. března 2026

Vedle států dnes kyberprostor formuje ještě jeden velmi silný aktér — organizovaná kyberkriminalita.

# Kyberkriminalita jako globální průmysl

- Škody způsobené kyberkriminalitou dosáhly v roce 2025 přibližně 10,5 bilionu dolarů.
- Pokud by kyberkriminalita byla státem, šlo by o třetí největší ekonomiku světa – hned po USA a Číně.
- **Až 68 % bezpečnostních incidentů začíná lidskou chybou.**
  - Phishing
  - Sociální inženýrství
  - Krádež přihlašovacích údajů

Forbes

Chci členství

Investice Průmysl Společnost Technologie Žebříčky Speciály Komentáře Woman Podcasty Newslettery Event

— Lepší Česko

## Kyberkriminalita už je třetí největší ekonomika světa, říká Majer z Respectu



Jana Divinová

+ [Odebírat autora](#)

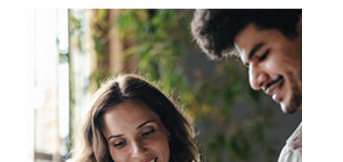
30. 10. 2025 ⌚ 3 min

📄 Sdílet 📌 Uložit

Když se firma stane obětí hackerů, nejde jen o výkupné. Jde o to, jestli přežije. Josef Majer z pojišťovací společnosti Respect na konferenci **Forbes Lepší Česko 2025** upozornil, že kybernetická kriminalita už dávno není parta kluků v kapucích. Dnes jde o miliardový byznys řízený jako korporace, a otázka nezní, jestli vás někdo napadne, ale zda budete připraveni, až to přijde.

Úspěch

mít kancelář, I  
přízpůsobí va



## Březen 2026: rekordní měsíc kyberkriminality v ČR

- nejhorší měsíc v historii (Policie ČR)
- 2 533 případů za jeden měsíc
- +37 % meziročně
- od začátku roku: 6 322 případů
- škody: stovky milionů Kč
- nejčastější oběti: **lidé 35–55 let**

### Nárůst kyberkriminality v Česku je rekordní, bije na poplach policie



Miloslav Fišer, ČTK

[vybrat autory ke sledování](#) ▼



2:58

Chcete-li článek poslouchat, [přihlaste se](#)

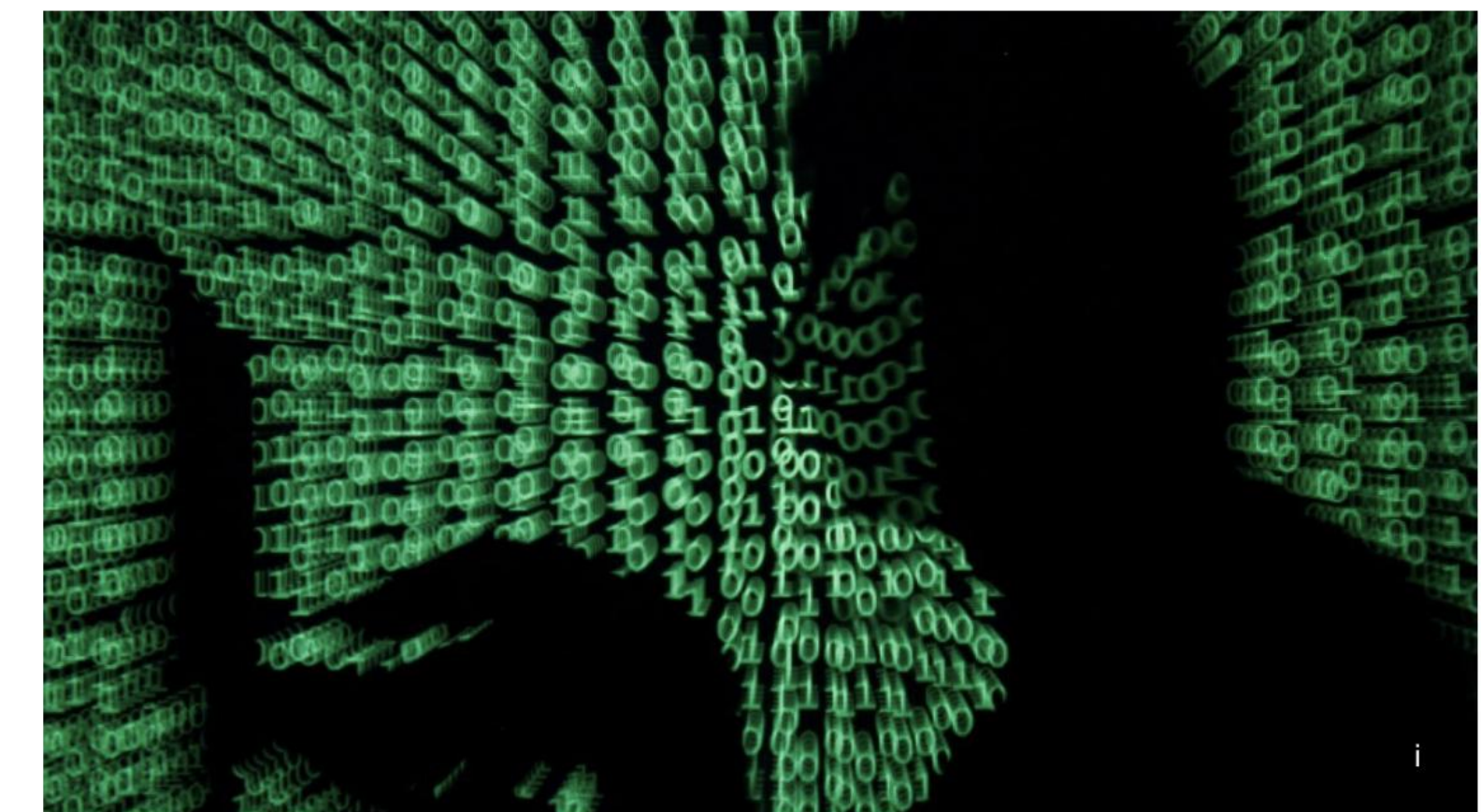
eBook

Sdílet

40

15. 4. 2026, 10:01

Případů kybernetické kriminality v březnu meziročně přibylo o 37 procent. Kriminalisté za březen evidují rekordních 2533 případů, řekl mluvčí Policejního prezidia ČR Ondřej Moravčík. Kyberšmejdi vypilovali své podvody skoro až k dokonalosti, i pro zkušené uživatele tak je velmi nesnadné je odhalit.



Ilustrační foto

Pro uživatele internetu jsou podle policistů nejrizikovější podvodní bankéři nebo policisté. Ti od začátku roku způsobili škodu za 322 milionů korun. Nejčastějšími oběťmi jsou ženy. Průměrný věk obětí je 46 let.

# Phishing a sociální inženýrství stále funguje

## WhatsApp device linking abused in account hijacking attacks

By **Bill Toulas**

December 17, 2025 02:14 PM 0



Gen Digital (formerly Symantec Corporation and NortonLifeLock) says that the campaign was first spotted in **Czechia** but warns that the propagation mechanism allows it to spread to other regions, with compromised accounts acting as springboards to reach new targets.



Threat actors are abusing the legitimate device-linking feature to hijack WhatsApp accounts via pairing codes in a campaign dubbed GhostPairing.

Zdroj: Bleeping Computer, Prosinec 2025

**CCTV CZECH CYBER TV** Hledat články... Zpravodajství O CCTV

**Jeden kód. Plný přístup.**  
*WhatsApp hlasovací podvod se šíří i mezi IT komunitou*

Ilustrační obrázek, vygenerováno ChatGPT

Novinky Článek

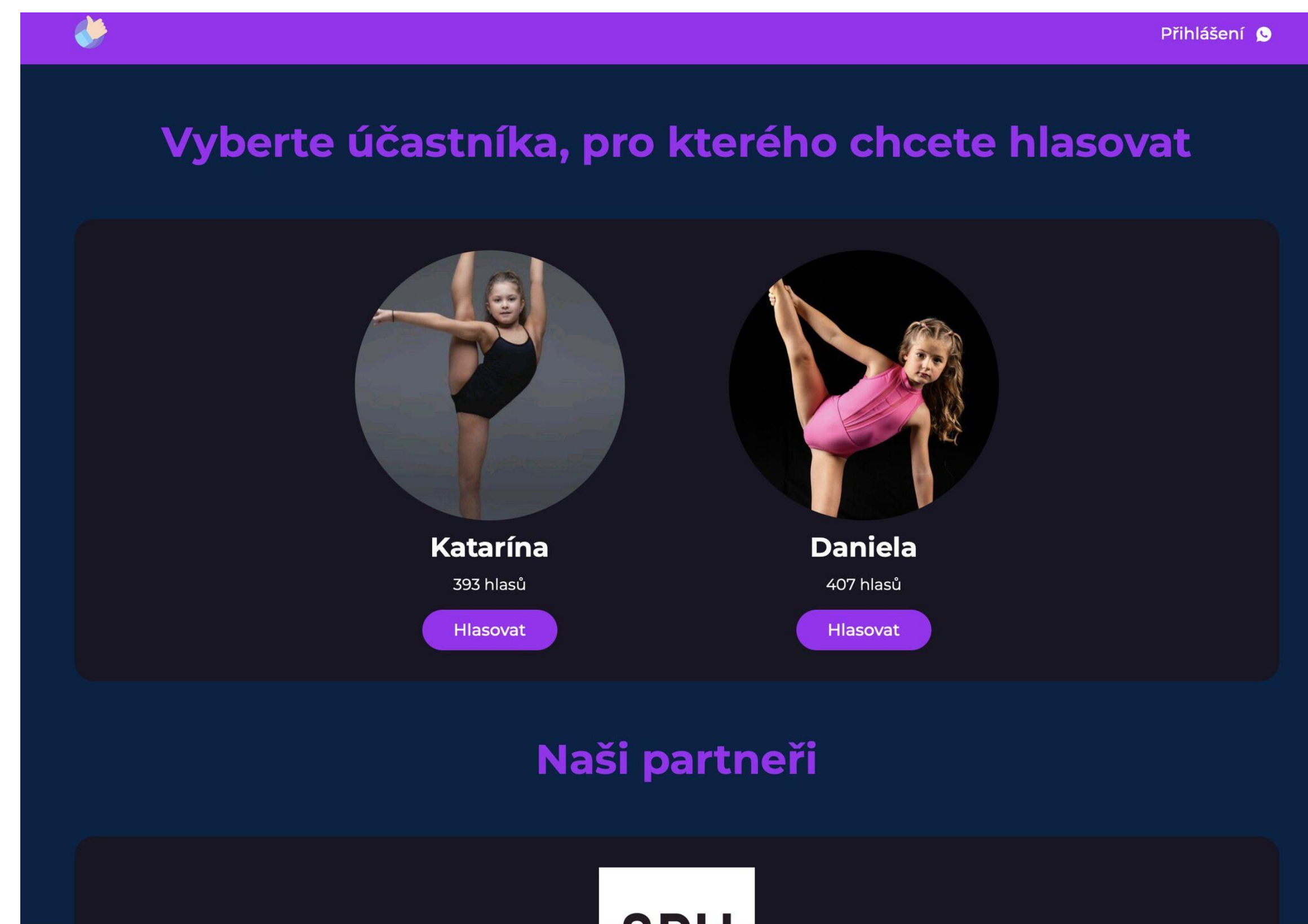
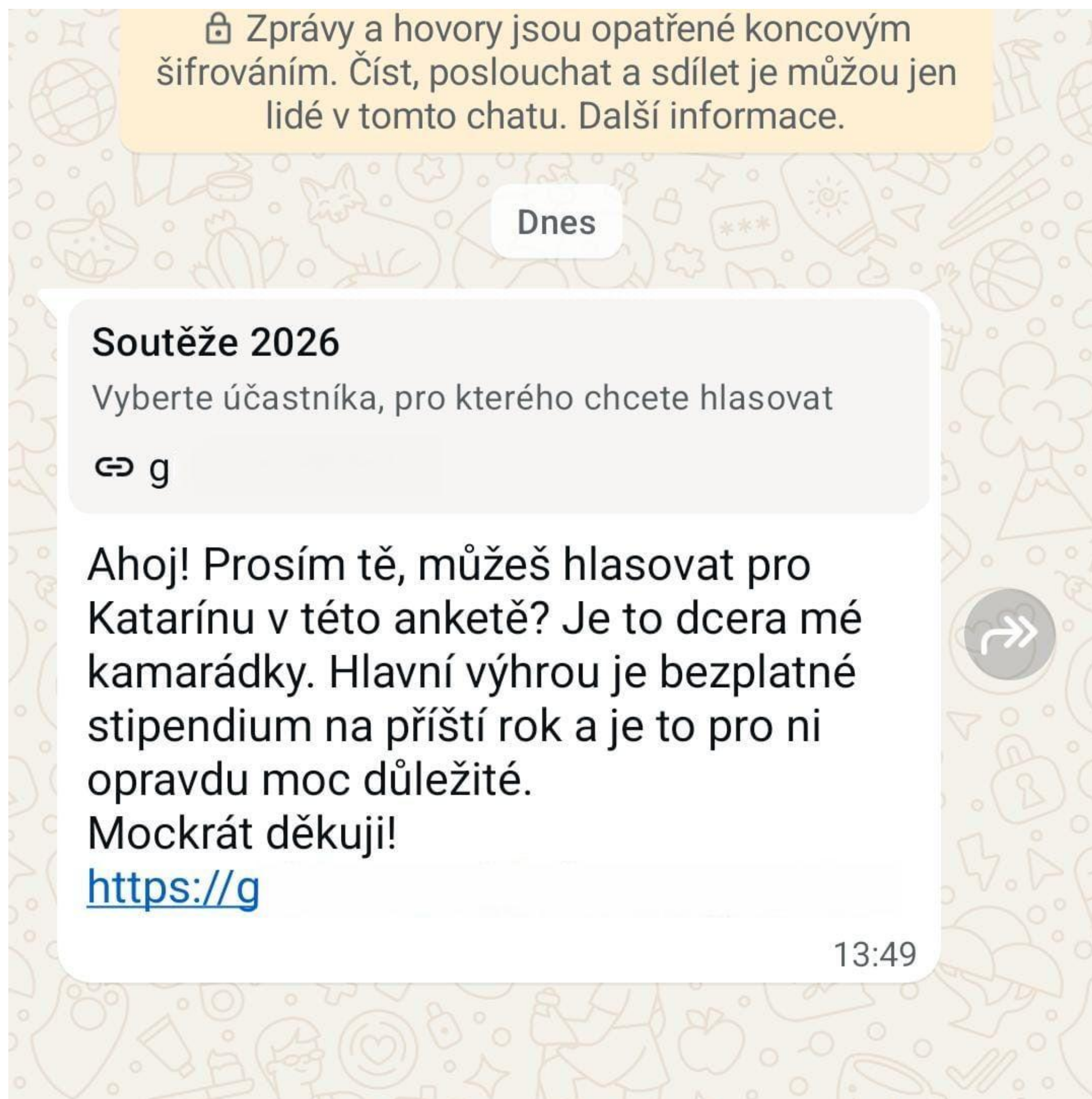
### Podvodné hlasování na WhatsAppu se šíří i mezi IT profesionály. Stačí jeden kód a útočník převezme celý WhatsApp účet

V posledních dnech se v českém prostředí výrazně šíří phishingová kampaň zaměřená na uživatele WhatsAppu. Zpráva přichází od důvěryhodného kontaktu a žádá o „hlasování v soutěži“ pro dceru známého. Odkaz vede na stránku, která působí jako běžná anketa, ve skutečnosti je však součástí promyšleného mechanismu převzetí účtu.

Stanislav Novotný | 2. března 2026

Zdroj: CZECH CYBER TV, Březen 2026

# Phishing a sociální inženýrství stále funguje



Co si z toho odnést

AI zrychluje kybernetické útoky  
i obranu

Kyberprostor je součástí geopolitiky

Většina útoků stále začíná lidskou  
chybou

Pokud vás tyto události zajímají, snažíme se je pravidelně mapovat na CZECH CYBER TV.



[CZECHCYBER.TV](http://CZECHCYBER.TV)



Spolufinancováno  
Evropskou unií

Ministerstvo životního prostředí

UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM



# **OSVĚTOVĚ ODBORNÝ VZDĚLÁVACÍ PROGRAM V OBLASTI KYBERNETICKÉ BEZPEČNOSTI**

vzdělávací akce realizovaná v rámci projektu  
CZ.10.02.01/00/22\_002/0000210, Aktivita KA1\_B.3.10  
RUR – Region univerzitě, univerzita regionu



RUR - Region univerzitě, univerzita regionu  
reg. č. CZ.10.02.01/00/22\_002/0000210

