Zimní olympijské hry 2026: kybernetická rizika významné události

5.2.2026 - | Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost upozorňuje v souvislosti s konáním zimních olympijských her na očekávatelnou větší aktivitu kyberútočníků a doporučuje institucím i jednotlivcům zvýšenou obezřetnost při aktivitách na internetu i ochranu vlastních zařízení.

V souvislosti s konáním zimních olympijských her (ZOH) 6.-22. února 2026 v italském Miláně a Cortině d'Ampezzo upozorňuje Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) na možné zvýšení aktivity kybernetických útočníků, zejména finančně motivovaných kriminálních skupin. Výraznými hrozbami zneužívajícími téma ZOH jsou phishingové kampaně, podvodné webové stránky a mobilní aplikace či QR kódy. Mezinárodní charakter a vysoká mediální pozornost ale mohou představovat atraktivní příležitost pro různé skupiny kyberútočníků: vyloučit nelze činnost hacktivistů ani útoky státem sponzorovaných aktérů.

„Stejně jako u jiných významných událostí i tady lze očekávat, že útočníci mohou využívat tematiku olympijských her k podvodům. Budou šířit podvodné e-maily a zprávy, které mají působit jako informace o vstupenkách, dopravě, ubytování nebo oficiálních organizačních pokynech. Využívají pocitu naléhavosti a pobízejí k rychlému, emocionálnímu, neuváženému rozhodování. Mohou se objevovat také falešné webové stránky, podvodné aplikace či QR kódy," upřesňuje některá kyberbezpečnostní rizika velkých událostí náměstkyně ředitele NÚKIB Martina Ulmanová.

Ačkoli NÚKIB zatím na území České republiky incident přímo související se ZOH 2026 nezaznamenal, existuje reálná možnost, že k tomu dojde. Olympijské hry se už v minulosti terčem kybernetických aktérů staly: V roce 2018 došlo k rozsáhlému kyberútoku, který ochromil IT infrastrukturu her v Pchjongčchangu. Olympiáda v Tokiu 2021 čelila snahám o sabotáž ze strany státem sponzorovaných útočníků. Letní olympijské hry v Paříži 2024 zaznamenaly 140 kybernetických incidentů, včetně 42 potvrzených dezinformačních kampaní a útoků využívajících deepfakes.

NÚKIB doporučuje, aby organizace i jednotlivci věnovali zvýšenou pozornost ověřování pravosti elektronické komunikace a vyvarovali se otevírání odkazů či příloh z neznámých nebo podezřelých zdrojů. Současně je důležité pravidelně aktualizovat používaný software, využívat vícefaktorové ověřování nebo místo veřejné wifi sítě raději využívat mobilní data.

Celý situační report, včetně dalších tipů, jak se kyberbezpečně chovat, naleznete zde: https://nukib.gov.cz/download/publikace/analyzy/Situacni-prehled-ZOH-2026.pdf

https://nukib.gov.cz/cs/infoservis/aktuality/2366-zimni-olympijske-hry-2026-kyberneticka-rizika-vyznamne-udalosti