ČNB: “Počet útoků na on-line bankovnictví se zvyšuje”. Hrozí kdykoli rozsáhlé výpadky online systémů a platebních karet. HOTOVOST JE NAPROSTO NEPOSTRADATELNÁ A JEJÍ POUŽITÍ BY MĚLO BÝT ZAKOTVENO V ÚSTAVĚ

- CZ24 News | 23. července 2023

ČESKO: Počet útoků v on-line bankovnictví v posledních letech několikanásobně narostl a stejně tak se zvyšuje i důmyslnost podvodů. Kriminalita páchaná v kyberprostoru za loňský rok představovala přes deset procent registrované kriminality v ČR. Cílovou skupinou útoků byla veřejnost včetně zranitelných skupin spotřebitelů. Útočníci používají hlavně podvodné telefonáty, takzvaný vishing, nebo podvržené odkazy v chatovacích aplikacích, textových zprávách nebo e-mailech, takzvaný phishing. Uvádí to Česká národní banka v pravidelné Zprávě o výkonu dohledu nad finančním trhem za loňský rok.

“Vysoký stupeň digitalizace finančních služeb přinesl v roce 2022 zesílené riziko podvodů v on-line prostředí, zejména v souvislosti s poskytováním platebních služeb, což je spojeno s dlouhodobým růstem kybernetické kriminality jako takové,” upozornila ČNB. Trestných činů páchaných v kyberprostoru podle dřívějších informací policejního prezidia v České republice loni meziročně přibylo 9036, bylo jich 18.554, tedy téměř o 100 procent víc než v předešlém roce.

Útočníci nejčastěji manipulativními technikami přiměli oběti ke sdělení osobních bezpečnostních prvků nebo k připojení podvodného zařízení k jejich účtu. Mohli tak odčerpat peníze z těchto účtů a v některých případech využili i další služby, například si sjednali spotřebitelský úvěr. Podvody se nejčastěji staly za součinnosti podvedených klientů, upozornila centrální banka. Klienti často sdělili své přístupové údaje potřebné pro uskutečnění platebních transakcí.

Náměstek policejního prezidenta Tomáš Kubík již dříve popsal, že pachatelé kybernetické kriminality u obětí například vyvolávají strach nebo zvědavost, zneužívají jejich důvěru, neznalost i časovou tíseň a zaštiťují se falešnými autoritami. Strach podle něj vyvolávají tak, že jim vyhrožují nebo je klamou ohledně toho, že při nečinnosti je čeká postih. Časovou tíseň stupňují tvrzením, že jejich nabídka je časově omezená.

“Proto je klíčové, aby finanční instituce důsledně a pravidelně informovaly své klienty o aktuálních hrozbách v souvislosti s poskytováním finančních služeb a o opatřeních, která sami klienti mají přijmout za účelem ochrany svých peněžních prostředků a následné prevence škod v případě, že se stanou obětí podvodu,” doporučuje ČNB.

Na nebezpečí útoků na klienty bank poukázal ve své zprávě za loňský rok i finanční arbitr. Uvedl, že nejčastějším typem sporů z platebního styku, který musel řešit, byly spory z neschválených platebních transakcí. Šlo podle něj zpravidla o falešné telefonáty nebo zneužití hesel. Také arbitr uvedl, že v některých případech si útočník sjednal s bankou spotřebitelský úvěr ve výši statisíců korun a peníze ukradl.

ČNB ve své zprávě doplnila, že vzhledem k nárůstu kybernetických rizik v důsledku eskalace geopolitické situace se zaměřila na podporu kybernetické odolnosti bank a dalších úvěrových institucí i finančního sektoru jako celku.

Problematikou kyberkriminality se od letošního roku zabývá nový policejní útvar, Národní centrála pro boj s terorismem, extremismem a kybernetickou kriminalitou (NCTEKK).

ZDROJ: ČNB/ČTK