

**Krajský úřad Jihočeského kraje
odbor ekonomický**

**DOPORUČENÁ PRIORITNÍ OPATŘENÍ PRO OCHRANU PLATEBNÍHO STYKU
PŘED PODVODNÝM JEDNÁNÍM**

Číslo informace:	11/2026/5/OEKO
Dotčená oblast:	kyberbezpečnost
Přehled právních předpisů, kterých se informace týká:	–
Určeno pro:	obce, dobrovolné svazky obcí a obecní příspěvkové organizace na území Jihočeského kraje
Platnost:	19. 8. 2026
Účinnost:	19. 8. 2026
Počet příloh:	–
Informace mění/zrušuje:	–
Vypracoval:	Ing. Aleš Zajac

S ohledem na množící se pokusy o podvodné telefonické vylákání plateb pod různými záminkami a další hybridní kybernetické útoky a s ohledem na to, že terčem jsou i příspěvkové organizace, je vydáno toto upozornění, které se vztahuje k zasílání elektronických plateb. Je v přímé odpovědnosti statutárního zástupce organizace, aby byly zavedeny takové vnitřní kontrolní mechanismy, které zamezí možnému zaslání platby na základě podvodných telefonátů nebo e-mailů. Mezi hlavní opatření, která lze doporučit zavést do kontrolních mechanismů před zasláním platby, patří:

(1) Dvoukroková a dvojitá autorizace plateb

Žádná platba by neměla být provedena bez schválení dvěma různými osobami. Při provádění plateb by měla být požadována autorizace dvou různých osob oprávněných disponovat peněžními prostředky. Každá osoba oprávněná disponovat peněžními prostředky musí mít vlastní přístup do internetového bankovníctví a potvrzení plateb probíhá přes telefon (smartbanking, smart klíč, George apod.) nebo jinou ověřovací metodou. Platbu lze provádět jen na základě účetního dokladu, resp. podkladu k finanční transakci, který musí být odsouhlasen odpovědnou osobou. Bez souhlasného stanoviska odpovědné osoby nelze provádět žádné platby, a to ani v situaci, která se jeví jako kritická (např. častým smyšleným důvodem je napadení bankovního účtu, kdy je nutné peněžní prostředky ihned převést jinam, volající se vydává za policistu, pracovníka banky apod.).

(2) Zpětné ověřování neobvyklých požadavků

Pokud někdo požádá o neobvyklou platbu nebo citlivé údaje, např. i ze strany statutárního zástupce, požadavek by měl být ověřen zpětným voláním na oficiální číslo dané instituce nebo osoby. Nikdy nelze používat číslo, které volající sám sdělí. Organizaci se doporučuje mít předem připravený seznam telefonních čísel pro zpětné ověření – např. na místní oddělení Policie ČR, banku, zřizovatele. Odpovědní zaměstnanci by měli mít tato telefonní čísla k dispozici.

(3) Platby pouze na základě schváleného podkladu v rámci finanční kontroly

Platba by měla být vždy zadávána z ekonomického systému (pokud ho organizace má), platby přímo zadávané do elektronického bankovníctví příslušné banky je doporučeno realizovat pouze výjimečně.

U plátců DPH je nutné ověřovat jejich spolehlivost a účty zveřejněné na portálu Finanční správy v Registru DPH.

(4) Okamžité hlášení incidentů

Každý zaměstnanec je povinen ihned nahlásit podezřelý e-mail, hovor, požadavek na platbu nebo nestandardní chování internetového bankovníctví nadřízenému a pověřené osobě pro bezpečnost/IT. Incident týkající se napadení bankovního účtu organizace VŽDY nahlásí bance a řídí se výhradně pokyny banky z ověřeného spojení na banku. Ředitel organizace by měl bezodkladně informovat svého zřizovatele.

(5) Limity pro platby

V bance je vhodné racionálně nastavit, s ohledem na každodenní potřeby organizace, maximální částku pro jednu platbu, denní limit pro odchozí platby, maximální limity pro platby přes internet nebo platební kartou k účtu.

(6) Řízení rizika okamžitých plateb

Při platbách je doporučeno používat standardní (nikoliv okamžité) převody, aby byla delší lhůta pro ověření a případné zastavení transakce. Lze tedy doporučit termín pro nastavení splatnosti a provedení platby minimálně na následující pracovní den.

(7) Školení zaměstnanců a testy ostražitosti

Doporučuje se pravidelně (alespoň 2× ročně) školit všechny osoby oprávněné k přípravě nebo schvalování plateb, pravidelně provádět testy např. v podobě simulace falešných e-mailů/telefonátů.

Prosíme zřizovatele o distribuci této informace svým příspěvkovým organizacím.