10. 10. 2019

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Silné ověření uživatele

Dne 14. září 2019 vešlo v účinnost nařízení Komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů (dále jen „Nařízení"). Směrnice Evropského parlamentu a Rady (EU) 2015/2366 (dále jen „PSD2")[1] byla do českého právního řádu transponována zákonem č. 370/2017 Sb. o platebním styku, a to s účinností od 13. ledna 2018 (dále jen „zákon o platebním styku").

Nařízení představuje přímo použitelný předpis ve smyslu ust. § 223 odst. 5 zákona o platebním styku, který stanoví způsob silného ověření, a jímž se provádí čl. 98 PSD2.

Faktory silného ověření

Silné ověření nebo také autentizace uživatele (SCA – *Strong Customer Authentication*) představuje bezpečnostní mechanismus, jehož cílem je eliminovat riziko platebních podvodů a jiných zneužití v důsledku kompromitovaného hesla. Jeho podstatou je ověření uživatele pomocí nejméně dvou prvků resp. faktorů.

Tyto faktory lze rozčlenit do tří kategorií:

- **Znalost**: prvek spočívající v určité znalosti uživatele (např. heslo, PIN, odpověď na kontrolní otázku);
- **Držba**: prvek spočívající v něčem, co má uživatel ve své moci (např. platební karta, mobilní telefon, fyzický token);
- **Inherence**: prvek reprezentující samotného uživatele, resp. to, čím je, typicky se jedná o biometrické údaje (např. otisk prstu).[2]

Kombinace nejméně dvou prvků dá vzniknout unikátnímu kódu, jenž má sloužit k silnému ověření uživatele.

Kdy se silné ověření použije

Silné ověření uživatele je vyžadováno v případech, které jsou vymezeny alternativním výčtem v ust. § 223 odst. 1 zákona o platebním styku:

„Osoba oprávněná poskytovat platební služby použije silné ověření uživatele, jestliže plátce

- *přistupuje ke svému platebnímu účtu prostřednictvím internetu,*
- *dává platební příkaz k elektronické platební transakci,*
- *provádí jiný úkon, který je spojen s rizikem podvodu v oblasti platebního styku, zneužitím platebního prostředku nebo informací o platebním účtu, nebo*
- *požaduje informace o platebním účtu prostřednictvím poskytovatele služby informování o platebním účtu.“*

Požadavek na silné ověření uživatele má tedy místo v těch situacích, kdy uživatel není v přímém kontaktu s poskytovatelem platebních služeb.[3] Jak se podává se shora citovaného výčtu, silné ověření uživatele se vyžaduje nejen při platebním příkazu k elektronické platební transakci a platbách v internetovém bankovnictví, ale již při samotném přístupu resp. přihlášení do internetového bankovnictví.

V navazujícím ust. § 223 odst. 2 zákona o platebním styku jsou dále zakotveny dodatečné požadavky na silné ověření uživatele, které se uplatní v případě, kdy je platební příkaz zadáván prostřednictvím internetu, elektronického zařízení, jež lze použít k dálkové komunikaci (typicky mobilní telefon), nebo je-li platební příkaz dáván nepřímo. [4]

Je nasnadě, že elektronické platební operace na dálku se pojí s vyšším rizikem platebního podvodu či jiného zneužití, dodatečné požadavky tak cílí na dosažení tzv. dynamického propojení transakce s částkou a příjemcem.[5] Pro tyto případy musí silné ověření uživatele zahrnovat rovněž jednorázové prvky propojující platební transakci s přesnou částkou a určitým příjemcem.

Implementace mechanismu silného ověření uživatele

Živá diskuse vyvstala v souvislosti s bezkontaktními platbami kartou, při nichž uživatel fyzicky přikládá kartu k platebnímu terminálu, a dále s využíváním internetového bankovnictví prostřednictvím mobilního telefonu, kdy se k autentizaci používá unikátní kód v ověřovací SMS zprávě.[6] Absence druhého ověřovacího prvku je ve zmíněných případech zřejmá.

Evropský orgán pro bankovnictví (dále jen „**EBA**“) ve stanovisku z června 2019 konstatoval, že zachování možnosti uživatelů platit, a to i on-line, má být při implementaci silného ověřování klíčová.[7] V zájmu eliminace negativních dopadů na uživatele platebních karet v prostředí e-commerce proto mohou orgány národního dohledu poskytnout na plnou implementaci mechanismu silného ověření uživatele dodatečný čas – leč v míře omezené.

Zmíněná benevolence je nicméně podmíněna přípravou a realizací implementačních plánů. Délka tohoto omezeného časového úseku má být konkretizována v rozhodnutí EBA, a to v následné reflexi údajů o situaci v jednotlivých členských státech EU a EHP.

Závěr

Dodržování nových pravidel bude samozřejmě podléhat dohledu ČNB, jež se ve věci silného ověřené uživatele vyjádřila mj. ve svém Sdělení v souvislosti s účinností nařízení Komise v přenesené pravomoci (EU) 2018/389. ČNB v duchu zmíněného stanoviska EBA deklarovala, že při své dohledové činnosti zohlední lhůtu či lhůty pro plnou implementaci Nařízení poté, kdy o nich EBA rozhodne. Je však třeba mít na paměti, že poskytnutí dodatečného času plnou implementaci silného ověření uživatele se nevztahuje na jiné karetní platby (např. karetní platby prostřednictvím terminálů pro jejich akceptaci), na něž tato povinnost dopadá.[8]

Mgr. Monika Gardlíková

DUNOVSKÁ & PARTNERS s.r.o., advokátní kancelář

Palác Archa
Na Poříčí 1046/24
110 00 Praha 1

Tel.: +420 221 774 000
e-mail: office@dunovska.cz

---

[1] PSD2 (*Payment Services Directive*) je druhá směrnice EU o platebních službách.

[2] Zde je nicméně třeba pamatovat na to, že biometrický údaj, jehož definice je zakotvená v článku 4 odst. 14 GDPR, představuje citlivý osobní údaj ve smyslu článku 9 GDPR, jehož zpracování podléhá zvláště přísným podmínkám.

[3] Důvodová zpráva k vládnímu návrhu zákona o platebním styku. Sněmovní tisk 1059/0, 2017.

[4] Nepřímé udělení platebního příkazu je platební službou definovanou v ust. § 2 odst. 1 písm. k) zákona o platebním styku, jež spočívá v dání platebního příkazu k převodu peněžních prostředků z platebního účtu jménem plátce poskytovatelem rozdílným od poskytovatele, který pro plátce vede daný platební účet, je-li platební příkaz dán prostřednictvím internetu.

[5] Srov. bod 3 Nařízení.

[6] Dle Pokynů Evropského bankovního orgánu (EBA) z 13. června 2018 se za prvek znalosti považuje něco, co uživatel zná, a tudíž číslo karty s datem exspirace a CVV kódem za prvek znalosti mít nelze.

[7] *Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2*, k dispozici >>> zde.

[8] Sdělení v souvislosti s účinností nařízení Komise v přenesené pravomoci (EU) 2018/389 k dispozici >>> zde.

Další články:

- Reklamace vad stavby
- Hodnotící dotazníky jako obchodní sdělení v kontrolním plánu ÚOOÚ pro rok 2026

- Konec „severních ateliérů“? Nový stavební zákon otevírá dveře k rekolaudaci ubytovacích jednotek na plnohodnotné byty
- Byznys a paragrafy, díl 33.: Prevence střetu zájmů (jednatel × společnost)
- Jak se vyhnout zákazu a postihu dohod o určování cen pro další prodej?
- Střet zájmů členů volených orgánů obchodních korporací: pravidla, proces a následky
- Nová „tlačítková” povinnost pro e-shopy
- Digital Omnibus: Revoluce v datech, nebo jen nová zátěž pro podnikatele?
- Právní due diligence nemovitostí: na co se v praxi skutečně zaměřit
- Hmotněprávní opatrovník obchodní korporace: mezi efektivní ochranou a zásahem do korporační autonomie
- Zákon Lugového: jak Rusko přepisuje pravidla mezinárodních arbitráží