Deloitte.

PSD2: Finální verze RTS k SCA - shrnutí zásadních změn

11. prosince 2017

1 Změny popsané v důvodové zprávě

1.1 Nová výjimka z aplikování SCA

(Article 17 Secure corporate payment processes and protocols)

Evropská komise doplnila další výjimku z aplikování silného ověření klienta, která se týká elektronických transakcí prováděných prostřednictvím vyhrazených platebních procesů nebo protokolů, které obvykle používají **korporátní společnosti (nikoliv spotřebitelé)** a **kde je zabezpečení dosaženo jinými prostředky než autentizací jednotlivé osoby**. Pro aplikování této výjimky používané platební metody mají dosahovat vysoké úrovně zabezpečení odpovídající nárokům ze strany příslušných orgánů.

1.2 Používání výjimek z aplikování SCA

Vzhledem k tomu, že osvobození od aplikování SCA prováděné na základě analýzy rizika transakcí je založeno na dodržování předem stanovených RFR (Reference fraud rate), je vhodné, aby přiměřenost mechanismu sledování úrovně podvodu poskytovatele platebních služeb byla podrobena kontrole ze strany **statutárního auditora,** jehož účelem je zajištění nestranného posouzení správnosti údajů.

Dosažené RFR by měly být nejen hlášeny příslušným orgánům za účelem zajištění účinného prosazování výjimek, ale měly by být **hlášeny také přímo EBA**, což jí umožní provést přezkum referenčních parametrů podvodů v RTS do 18 měsíců po vstupu RTS v platnost.

1.3 Anonymní platební nástroje

SCA není vynucováno při platbách uskutečněných prostřednictvím anonymních platebních nástrojů, a o s ohledem na jejich povahu. Je samozřejmé, že v případě, kdy by byla jejich anonymita zrušena, stanou se i tyto platby předmětem povinné aplikace SCA.

1.4 Screen scraping bude zakázán

Ode dne účinnosti RTS nebude ‘screen scraping’ možné používat v podobě, v jaké je používán v současnosti, bude totiž v rozporu s podmínkami nastavenými právě předmětnými RTS.

1.5 Vyhrazené rozhraní (dedicated interface)

(Article 32 Obligations for a dedicated interface**,** Article 33 Contingency measures for a dedicated interface)

RTS nařizuje, že pokud se ASPSP (tedy banka) rozhodne použít vyhrazené rozhraní, musí pro toto rozhraní definovat transparentní **klíčové ukazatele výkonnosti (KPI) a cíle úrovně služeb (Service level targets)**. KPI a cíle úrovně služeb musí být přinejmenším stejně přísné jako ty, které jsou nastaveny pro rozhraní používané uživateli platebních služeb ASPSP. Data musí být zveřejňována čtvrtletně. (článek 32, odst. 2 RTS - SCA)

Aby nedocházelo k nedostatečnému výkonu vyhrazeného rozhraní bránícímu TPP poskytovat své služby uživatelům, v situaci kdy uživatelsky orientované rozhraní fungují bez jakýchkoli potíží a umožňují ASPSP nabízet své vlastní služby, komise zavedla **opatření ve formě nouzových mechanismů**, které spočívají v otevření uživatelsky orientovaných rozhraní jako bezpečného komunikačního kanálu pro služby třetích stran.

Deloitte.

Komise pověřila příslušné vnitrostátní orgány, aby **osvobodily banky od povinnosti poskytovat nouzové mechanismy při splnění přísných podmínek**, zaručujících, že vyhrazená rozhraní skutečně otevřou trh platebních služeb. (článek 33, odst. RTS - SCA6)

Vyhrazená rozhraní mají být otestována poskytovateli platebních služeb, kteří je budou používat. Kromě toho vyhrazená rozhraní budou podrobena **zátěžovému testování a monitorování příslušnými orgány**. V případě, že se tato vyhrazená rozhraní neprojdou testovací fází nebo nevyhoví zátěžovým testům, poskytovatelé platebních služeb budou moci využít tzv. nouzový mechanismus. (článek 32, odst. RTS - SCA 2).

Pro případy, kdy je vyhrazené rozhraní vyňato z nouzového mechanismu na základě uživatelského rozhraní, ale již nesplňuje požadavky na takovou výjimku nebo případy, kdy ASPSP nenabízí žádné rozhraní vyhovující požadavkům PSD2 a RTS, zavedla Komise ustanovení zajišťující kontinuitu činností v oblasti realizace platebních příkazů. V takovém případě příslušné orgány zajistí, aby PISP a AISP nebyly zablokovány a nebylo jim bráněno v poskytováních jejich služeb. (článek 33, odst. 7 RTS – SCA).

2 Další změny

#	Popis	Finální RTS	Související odstavec v draft verzi RTS
1	Do **minimálních risk-based faktorů** sledovaných mechanismem monitorování transakcí je nově přidáno **vyhodnocování logu o používání přístupového zařízení nebo softwaru** poskytnutého uživateli platebních služeb a abnormální použití přístupového zařízení nebo softwaru, v případě, že přístupové zařízení nebo software je poskytnuté poskytovatelem platebních služeb.	čl. 2(2)	čl. 2(3) dříve bylo v rámci real-time mechanismu pro TRA
2	Nově je přesně uvedeno, že hodnocení a audit bezpečnostních metod musí být proveden **auditory s odbornými znalostmi v oblasti IT bezpečnosti a plateb** a **operativně nezávislými** od poskytovatele platebních služeb.	čl. 3(1)	čl. 3(1) dříve auditoři měli být interní nebo externí nezávislí a kvalifikovaní
3	Při používání výjimky z aplikování SCA na základě TRA (čl. 18) musí být audit proveden **během prvního roku a poté nejméně jednou za tři roky nebo častěji na žádost příslušného orgánu, a to nezávislým a kvalifikovaným externím auditorem**.	čl. 3(2)	čl. 3(2) dříve tato povinnost nebyla
4	Nově je používána formulace „**shall be allowed** not to apply strong customer authentication", čímž je odstraněno předchozí zavádějící vyjádření.	čl. 10-18	čl. 10-16 dříve bylo „are exempted"
5	Přeformulován článek 10 - Payment account information. čl. 10(2b): *„more than 90 days have elapsed since the last time the payment service user accessed online the information specified in paragraph 1(b) and strong customer authentication was applied."*	čl. 10	čl. 10
6	Pozor, celková míra podvodů musí být počítána a být menší nebo rovna referenční míře podvodu u každé provedené transakce, jak při SCA tak i bez SCA.	čl. 19	čl. 16 dříve bylo špatně zařazeno do článku 16
7	ASPSP musí **zpřístupnit dokumentaci** technické specifikace rozhraní nejméně **šest měsíců** před datem účinnosti RTS nebo datem uvedení přístupového rozhraní na trh, pokud se zahájení uskuteční po datu účinnosti.	čl. 30(3)	čl. 27(4)
8	ASPSP musí **zpřístupnit testovací prostředí** (Testing facility) nejméně **šest měsíců** před datem účinnosti RTS nebo datem uvedení přístupového rozhraní na trh, pokud se zahájení uskuteční po datu účinnosti.	čl. 30(5)	čl. 27(6)
9	**Příslušné orgány musí zajistit**, aby banky (ASPSP) vždy splňovaly povinnosti ve vztahu k rozhraním, která zavedly. V případě, že ASPSP nesplňuje stanovené požadavky na rozhraní, příslušné orgány musí zajistit, aby nebylo zabráněno nebo narušováno poskytování TPP služeb.	čl. 30(6)	Nové

Deloitte.

10	Za neočekávanou **nedostupnost nebo poruchu systému** lze považovat **neodpovídání na pět po sobě jdoucích žádosti** o přístup TPP během **30 sekund**.	čl. 33(1)	čl. 28(4) nebylo definováno
11	ASPSP musí zajistit, že TPP může být identifikováno a může se spolehnout na autentizační postupy poskytované ASPSP uživatelům platebních služeb. Pokud TPP používají vyhrazená rozhraní, musí: a) přijmout nezbytná opatření k zajištění toho, aby nepřistupovali, neuchovávali nebo nezpracovávali údaje k jinému účelu než pro poskytování služby vyžadované uživatelem; b) nadále plnit povinnosti podle čl. 66 odst. 3 a čl. 67 odst. 2 směrnice (EU) 2015/2366; c) zaznamenávat (log) údaje, ke kterým TPP přístupová prostřednictvím rozhraní a na požádání bez zbytečného odkladu poskytnout záznamy (log) příslušnému vnitrostátnímu orgánu; d) řádně odůvodnit svému příslušnému vnitrostátnímu orgánu na žádost a bez zbytečného odkladu používání rozhraní, které je poskytováno uživatelům platebních služeb k přímému přístupu k jejich účtu on-line; e) informovat o tom ASPSP.	čl. 33(5)	Nové
12	Příslušné orgány musí **zrušit osvobození** ASPSP od povinnosti poskytovat nouzové mechanismy uvedené v čl. 33 odst. 6, pokud podmínky uvedené v písmenech a) a d) nejsou splněny ASPSP **déle než dva po sobě jdoucí kalendářní týdny**. Příslušné orgány musí informovat EBA o tomto zrušení a zajistit, aby ASPSP poskytl v co nejkratší možné době a nejpozději **do dvou měsíců** mechanismus pro nouzové události uvedený v čl. 33 odst. 4.	čl. 33(7)	Nové

Tomáš Huml
Manager, Financial Services & PSD2 Technology Advisory
Deloitte Advisory s.r.o.
thuml@deloittece.com
