10. 8. 2017

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

Nové povinnosti bank podle zákona o kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti („Zákon“), upravuje již od roku 2015 povinnosti některých orgánů a osob, zejména provozovatelů sítí elektronických komunikací, v oblasti předcházení kybernetickým bezpečnostním hrozbám. Dne 14. července 2017 byla ve Sbírce zákonů pod č. 205/2017 Sb. publikována novela Zákona („Novela“), jež je transpozicí směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii a v jejímž důsledku se budou s účinností od 1. srpna 2018 povinnosti v oblasti kybernetické bezpečnosti nově vztahovat na široké spektrum Zákonem dosud neregulovaných soukromoprávních subjektů, včetně bank. Jaké tedy budou nové povinnosti bank a za jakých podmínek se bude na banky vztahovat nová regulace?

GLATZOVA & Co.

Nové zákonné pojmy „základní služba“ a „provozovatel základní služby“

Základním cílem Novely je v souladu s požadavky evropského práva posílení bezpečnosti informačních systémů. Podle Novely je nově jedním z účelů Zákona zajišťování sítí elektronických komunikací a informačních systémů. V této souvislosti zavádí následující nové zákonné pojmy:

- (i) „základní služba“, kterou se rozumí služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností ve vymezených oblastech ekonomické činnosti, a to včetně oblasti bankovnictví [1];
- (ii) „informační systém základní služby“, kterým se rozumí informační systém, na jehož fungování je závislé poskytování základní služby („ISZS“); a
- (iii) „provozovatel základní služby“, kterým se rozumí osoba, která poskytuje základní službu a která je určena rozhodnutím Národního úřadu pro kybernetickou a informační bezpečnost („Úřad“).

Základní službou v oblasti bankovnictví se přitom podle důvodové zprávy k Novele rozumí výkon činnosti úvěrové instituce ve smyslu § 17a odst. 3 zákona č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, tedy výkon činnosti úvěrové instituce ve smyslu nařízení Evropského parlamentu a Rady (EU) č. 575/2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky. Jinými slovy, základní službou v oblasti bankovnictví ve smyslu Zákona je, mimo jiné, též výkon činnosti banky ve smyslu § 1 písm. a) a b) zákona o bankách.
Určení provozovatele základní služby v oblasti bankovnictví

Provozovatelem základní služby podle Zákona je pouze osoba určená rozhodnutím Úřadu. Podle § 22a Zákona určí Úřad rozhodnutím provozovatele základní služby a ISZS, pokud provozovatel naplní tzv. odvětvová a dopadová kritéria, která budou v podrobnostech stanovena novou prováděcí vyhláškou o určování provozovatelů základních služeb („Určovací vyhláška“). Podle tezí Určovací

vyhlášky, které jsou součástí návrhu Novely, musí být pro určení subjektu jako provozovatele základní služby naplněno (i) alespoň jedno dopadové určující kritérium a (ii) alespoň jedno odvětvové určující kritérium.

Dopadové určující kritérium je přitom naplněno v okamžiku, kdy narušení bezpečnosti informací v informačním systému a síti základní služby může způsobit některý z následujících dopadů: a) omezení základní služby postihující více než 50.000 – 100.000 osob; b) závažné omezení či narušení jiné základní služby, nebo omezení či narušení provozu prvku kritické infrastruktury; c) hospodářskou ztrátu vyšší než 250 – 500 milionů Kč; d) nedostupnost služby poskytované alespoň 50.000 – 100.000 osobám, která není nahraditelná jinou službou; e) oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1.000 zraněných osob vyžadujících lékařské ošetření; f) ohrožení veřejné bezpečnosti v minimálním rozsahu správního území obce s rozšířenou působností; či g) kompromitaci citlivých údajů o nejméně 200.000 osobách.

Odvětvovým určujícím kritériem v odvětví bankovnictví bude podle tezí Určovací vyhlášky minimální podíl úvěrové instituce na trhu. Prahová hodnota minimálního tržního podílu bude nastavena na základě výsledků jednání pracovní skupiny, sestavené ze zástupců věcně příslušných resortů, zástupců průmyslu a odborné veřejnosti, kterou Úřad svolá v průběhu projednávání Určovací vyhlášky.

Lze očekávat, že banky s nejvýznamnějšími podíly na bankovním trhu v České republice [2] budou rozhodnutím Úřadu určeny jako provozovatelé základní služby a jimi provozované systémy jako ISZS ve smyslu Zákona. V takovém případě budou tyto banky podle § 3 Zákona povinny plnit povinnosti provozovatele základní služby, resp. správce a provozovatele ISZS, jak vyplývají ze znění Zákona po Novele.

Povinnosti provozovatele základní služby

Povinnost zavést a provádět bezpečnostní opatření

Podle § 4 odst. 2 Zákona je správce a provozovatel ISZS povinen zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti ISZS a vést o nich bezpečnostní dokumentaci. Konkrétní požadavky na bezpečnostní opatření budou stanovena v novelizovaném znění vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

Povinnost zohlednit bezpečnostní opatření při výběru dodavatele

Podle § 4 odst. 4 Zákona je správce a provozovatel ISZS povinen zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jeho informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy uzavřené s dodavatelem.

Povinnost informovat správce ISZS o určení provozovatelem základní služby

Podle § 4a odst. 3 Zákona je osoba, která byla rozhodnutím Úřadu určena jako provozovatel základní služby a která není zároveň správcem nebo provozovatelem svého ISZS, povinna informovat správce nebo provozovatele tohoto ISZS o svém určení.

Povinnost detekovat a hlásit kybernetické bezpečnostní incidenty

Podle § 7 odst. 3 a § 8 odst. 1 Zákona je správce nebo provozovatel ISZS povinen detekovat kybernetické bezpečnostní incidenty v jeho ISZS, a bezodkladně po jejich detekci je hlásit Úřadu.

Provozovatel základní služby je navíc podle § 8 odst. 1 Zákona povinen oznámit Úřadu, zda kybernetický bezpečnostní incident má významný dopad na kontinuitu poskytování základní služby.

Povinnost provádět opatření Úřadu

Úřad je podle § 11 až 15a Zákona oprávněn vydávat opatření, kterými se rozumí varování, reaktivní opatření a ochranná opatření. Podle § 11 odst. 3 písm. b) a odst. 4 Zákona je správce nebo provozovatel ISZS povinen provádět jak reaktivní opatření Úřadu, tak ochranná opatření Úřadu.

V případě, že je správce nebo provozovatel ISZS dotčen kybernetickým bezpečnostním incidentem, je Úřad podle § 12 odst. 3 Zákona oprávněn tomuto správci nebo provozovateli ISZS po konzultaci s ním uložit povinnost informovat o tomto incidentu veřejnost. Podle důvodové zprávy k Novele bude v případě finančního sektoru, kde by informace o incidentu v rámci jedné banky mohla ovlivnit celý finanční sektor a způsobit dokonce i jeho kolaps, relevantní též stanovisko České národní banky.

Úřad ukládá reaktivní opatření buď správním rozhodnutím, nebo opatřením obecné povahy vyvěšeným na úřední desce Úřadu. Účelem reaktivního opatření je okamžitá reakce na výskyt kybernetického bezpečnostního incidentu a obsahem opatření tedy mohou být povinnosti provést konkrétní úkony nutné k odvrácení kybernetického bezpečnostního incidentu nebo ke zmírnění jeho následků. Provozovatel nebo správce ISZS je povinen bez zbytečného odkladu oznámit Úřadu provedení reaktivního opatření a jeho výsledek.

Ochranná opatření ukládá Úřad opatřením obecné povahy vyvěšeným na úřední desce Úřadu, kterým na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu stanoví způsob zvýšení ochrany a přiměřenou lhůtu k jeho provedení.

Povinnost oznámit Úřadu kontaktní údaje a jejich změny

Podle § 16 odst. 2 písm. b) Zákona oznamuje provozovatel základní služby, resp. správce nebo provozovatel ISZS Úřadu své kontaktní údaje, kterými se v případě právnické osoby rozumí obchodní firma, adresa sídla, identifikační číslo osoby a údaje o fyzické osobě, která je oprávněna za ni jednat, a to jméno, příjmení, telefonní číslo a adresa elektronické pošty.

Podle § 16 odst. 3 Zákona se ukládá povinnost ohlásit změny kontaktních údajů, avšak pouze těch, které nejsou vedeny jako referenční údaje v základních registrech.

Sankce za nedodržení povinností provozovatele základní služby

Úřad je oprávněn vykonávat kontrolu v oblasti kybernetické bezpečnosti a ukládat správci nebo provozovateli ISZS nápravná opatření podle § 24 Zákona a pokuty za přestupky podle § 25 odst. 7 a 10 Zákona.

Maximální výše pokut za porušení povinností správce nebo provozovatele ISZS, resp. provozovatele základní služby, podle Zákona se pohybují od 1.000.000 Kč (neohlášení kybernetického bezpečnostního incidentu, nesplnění reaktivních nebo ochranných opatření) až do 5.000.000 Kč (porušení povinnosti zavést a provádět bezpečnostní opatření).

Přechodná ustanovení novely – kdy bude určen provozovatel základní služby a kdy musí

začít plnit povinnosti dle novely?

Úřad je povinen určit provozovatele základní služby a ISZS nejpozději do 9. listopadu 2018. Správce nebo provozovatel ISZS je povinen oznámit Úřadu své kontaktní údaje do 30 dnů ode dne, kdy byl informován o určení provozovatele základní služby, resp. ode dne oznámení rozhodnutí, pokud je sám správcem a provozovatelem svého ISZS. Provozovatel základní služby, resp. správce nebo provozovatel ISZS, je poté povinen začít plnit ostatní povinnosti podle Zákona po Novele nejpozději do 1 roku ode dne, kdy byl informován o určení provozovatele základní služby.

Správce nebo provozovatel ISZS, resp. provozovatel základní služby, je dále povinen do 1 roku od nabytí účinnosti Novely uvést smluvní vztahy s jeho dodavateli do souladu se zněním zákona po Novele.

Závěr

Zákon se ve svém znění po Novele stává další veřejnoprávní regulací dopadající na banky a též na další soukromoprávní subjekty ze strategických ekonomických odvětví. Vnitřní procesy, předpisy a postupy bank, které budou rozhodnutím Úřadu určeny jako provozovatelé základní služby, tak budou muset být přizpůsobeny poměrně striktní nové úpravě Zákona, což bude zahrnovat mimo jiné zavedení a provádění bezpečnostních opatření, uvedení smluvní dokumentace s dodavateli do souladu se Zákonem, zavedení procesů pro detekci kybernetických bezpečnostních incidentů, pro adekvátní a včasné reakce na opatření Úřadu či pro provádění pravidelné interní kontroly správného fungování procesů spojených se zajištěním kybernetické bezpečnosti. I s ohledem na maximální možnou výši sankcí za porušení Zákona lze jen doporučit, aby banky věnovaly dostatečnou pozornost svým novým povinnostem v oblasti kybernetické bezpečnosti a odpovídající úpravě svých vnitřních procesů a předpisů.

Mgr. et Mgr. Filip Murár

Glatzová & Co., s.r.o.

Betlémský palác
Husova 5
110 00 Praha 1

Tel.: +420 224 401 440
Fax: +420 224 248 701
e-mail: office@glatzova.com

---

[1] Dalšími nově regulovanými odvětvími jsou energetika, doprava, infrastruktura finančních trhů, zdravotnictví, vodní hospodářství, digitální infrastruktura a chemický průmysl.
[2] Lze očekávat, že těmito bankami budou přinejmenším tzv. systémově významné instituce ve smyslu čl. 131 směrnice CRD IV a § 12w zákona o bankách, jejichž seznam je k dispozici na webu ČNB, dostupné na www, k dispozici >>> zde.

Další články:

- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- TOP 5 judikátů z korporátního práva za rok 2025
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- SCHEJBAL& PARTNERS stáli u získání jedné z prvních licencí dle MiCA v ČR
- Proč dnes více než polovina M&A transakcí ve střední Evropě nekončí podpisem
- Přehnaná, nebo důvodná prevence? Zajištění a utvrzení závazků v praxi
- Návrh nového zákona o digitální ekonomice
- Byznys a paragrafy, díl 30.: Jednání za s.r.o. – zápis jednatelského oprávnění do obchodního rejstříku
- Prověřování zahraničních investic a kybernetická regulace: řízená služba jako nová transakční proměnná
- Předběžné opatření a další instituty k ochraně věřitelů při přeměnách