TISKOVÁ ZPRÁVA

Evropská unie si posvítí na útoky hackerů a lépe zabezpečí finanční sektor

Ochránit banky, další finanční instituce a společně s tím i účty milionů lidí má za cíl evropská směrnice DORA závazná pro Česko i všechny ostatní členské státy. Evropská unie tak reaguje na narůstající počet kybernetických útoků. Pro finanční instituce proto nastavuje jasná pravidla, jak se mají před digitálními riziky chránit a jak mají případně postupovat, pokud by je nějaký útok skutečně zasáhl. Zásadní změna to bude zejména pro menší finanční instituce, které doposud tuto otázku řešit příliš nemusely, a pro dodavatelské řetězce. Co evropská směrnice konkrétně přinese, rozebírá v komentáři Michael Kralert, ředitel oddělení společnosti BDO, poskytující poradenské služby bankám, pojišťovnám a subjektům kapitálovému trhu.

Finanční instituce mají relativně krátkou dobu na zajištění souladu s regulatorními požadavky. Lhůta jim běží od 16. ledna 2023, kdy směrnice DORA (Digital Operational Resilience Act) vstoupila v platnost, a potrvá po dobu dvou let.

Směrnice stanovuje, že všechny společnosti spojené s finančním sektorem musí být schopny zabezpečit své informační a komunikační systémy proti případným narušením a hrozbám a v případě problémů okamžitě reagovat. Tyto přísné standardy budou muset respektovat nejen banky a ostatní finanční instituce, ale také třetí strany poskytující tomuto sektoru kritické služby související s informačními a komunikačními technologiemi, jako například poskytovatelé cloudových služeb. Celkově se bude jednat o tisíce firem.

Cílem směrnice je zabránit kybernetickým útokům, aby narušily digitální ochranu finančních institucí, případně snížení dopadu úspěšných pokusů o narušení. Směrnice přitom reaguje na vzrůstající rizika v podobě vyšší propojenosti finančního sektoru a nárůstu digitalizace, zaměřuje se přitom i na sjednocení dosavadního poměrně roztříštěného systému kontroly.

Největší těžkosti s přípravou mohou mít zejména menší finanční instituce

Významné bankovní instituce byly již dříve pod drobnohledem kontrolních orgánů, díky čemuž pro ně nová regulace nebude zásadní změnou. Naopak menší instituce ve finančním sektoru zpravidla čeká náročná příprava. Nařízená ochrana jejich odolnosti před hackery v takovém rozsahu bude pro většinu z nich novinkou a na zajištění souladu s regulací již nemají příliš času. Zároveň však mohou počítat s tím, že rozsah nutných opatření bude přímo úměrný jejich velikosti a rozsahu poskytovaných finančních služeb.

Všechny dotčené instituce budou muset průběžně plnit řadu stanovených úkolů. Nejde přitom pouze o technické aspekty bezpečnosti, na rozdíl do některých předchozích nařízení se DORA zaměřuje i na provozní aspekty.

Zásadní bude testování odolnosti, odhalování rizik a sdílení informací o hrozbách a incidentech
Konkrétně budou muset jednotlivé instituce podle regulace DORA zavést vhodné **řízení rizik** v tom smyslu, že identifikují zranitelná místa a posoudí všechna relevantní rizika spojená se svými digitálními provozními systémy a jejich vzájemnou provázaností. Rizikovost by měla být vyhodnocována průběžně, pravidelně přezkoumávána a aktualizována. Kromě snahy o zmírnění rizik by instituce měly průběžně transparentně vyhodnocovat stav rizikovosti.

Pro případ kybernetického útoku instituce mají mít důkladný plán řízení incidentů a reakce na ně, a to včetně předem vyhodnoceného schématu komunikace s příslušnými zúčastněnými stranami a nástrojů ke zmírnění dopadu incidentu. Soustředit se dále mají primárně na ochranu dat a kontinuitu provozu. Do celého procesu musí být začleněn i celý dodavatelský řetězec, na což DORA klade oproti dřívějším regulacím značně větší důraz.

Druhým zásadním úkolem pro finanční instituce je **hlásit incidenty** neprodleně příslušným státním orgánům. Informace by měla obsahovat údaj o délce incidentu, přehled o všech dotčených organizacích a geografický rozsah incidentu, zvláště pokud probíhal na území více než dvou členských států. Případně by instituce měly uvést, zdali útok způsobil ztrátu dat, či narušil jejich integritu, a kolika transakcí či jaké částky se incident dotkl. Doplnit by měly také, jestli incident způsobil dopad na pověst a jaký je jeho hospodářský dopad v odhadnutých přímých a nepřímých nákladech a ztrátách.

Dále DORA nařizuje dotčeným subjektům regulace, aby prováděly pravidelné **testování odolnosti** svých IT systémů a procesů s cílem zajistit jejich účinnost a identifikovat potenciální problémy. Zavedení účinných bezpečnostních kontrol může být pro organizace výzvou, protože musí zajistit, aby odpovídaly velikosti, složitosti a rizikovému profilu své digitální infrastruktury a služeb. Kromě toho musí organizace zajistit, aby všechny bezpečnostní kontroly byly pravidelně monitorovány a testovány.

Kromě toho DORA předpokládá vzájemnou kooperaci a **sdílení informací**. Nařizuje, aby finanční instituce sdílely informace s jinými finančními institucemi a regulačními orgány v jiných zemích, což může představovat výzvu z hlediska ochrany údajů, důvěrnosti a regulačních požadavků.

Přitom lze očekávat, že některé rutinní činnosti spojené s testováním, sběrem a zpracováním dat v souvislosti s reportingem budou brzy v budoucnu vykonávány s minimálním zapojením lidské činnosti, kterou nahradí strojové učení a umělá inteligence, a to i z toho důvodu, že firmy nebudou mít dostatek zaměstnanců, kteří by se vyhodnocování stále většího objemu dat mohli věnovat.

Odborníků na kyberbezpečnost bude nedostatek
Lze také očekávat, že odborníků, kteří by ještě předtím řešili samotnou implementaci regulace, bude nedostatek, stejně tak jako na druhé straně inspektorů nastavených procesů. Ostatně nouzi o odborníky zažívají firmy již nyní.

Zejména pro menší firmy se zdá nerealistické, že by dokázaly sestavit trvalý plnohodnotný tým odborníků na kybernetickou bezpečnost. Proto lze očekávat větší zapojení externích partnerů, případně lze očekávat zajišťování některých komponent kybernetické bezpečnosti určitou formou sdílené služby.

Přitom sháňka po odbornících na kybernetickou bezpečnost naroste nejen vlivem přicházející regulace DORA, ale i dalších směrnic týkajících se kybernetické bezpečnosti jako NIS2.

Z předlohy směrnice NIS2 vychází i vznikající zákon o kybernetické bezpečnosti, s jehož účinností česká legislativa předběžně počítá od druhé poloviny roku 2024 a který se dotkne tisíce českých firem. Na rozdíl od regulace DORA se ovšem týká vybraných klíčových subjektů napříč obory, zatímco DORA bude platná vyloženě pro finanční sektor. V případě rozporu u finančního sektoru, kterou směrnicí se má řídit, dostane vždy přednost DORA jakožto specifičtější zákonná úprava před NIS2.

Kdo bude předpis porušovat, čeká ho sankce

Příslušný státní orgán může v případě jakéhokoliv porušení regulace DORA uložit správní sankce a nápravná opatření, jejich výše pro finanční instituce nicméně zatím nebyla stanovena. Ovšem kritickým poskytovatelům informačních a komunikačních služeb mohou úřady uložit pokutu do 1 % jejich průměrného denního celosvětového obratu za předchozí hospodářský rok po dobu maximálně šesti měsíců, a to denně až do dosažení souladu s předpisy.

Jak finanční instituce, tak jejich dodavatelé by se měli na regulaci připravovat již v současné době. Lhůta, kterou na splnění zákonných podmínek mají, opravdu není příliš dlouhá.

Autor: *Michael Kralert, ředitel oddělení společnosti BDO*

TISKOVÁ ZPRÁVA

O společnosti BDO

BDO je poradenská společnost poskytující auditorské, daňové, právní, účetní a poradenské služby. Na českém trhu působí již 30 let. S téměř 500 odborníky a dlouholetou praxí se řadí k předním společnostem s tímto zaměřením v České republice, kde má kanceláře v Praze, Plzni, Brně, Domažlicích, Českých Budějovicích a Jindřichově Hradci.

BDO je v České republice zastoupena společnostmi BDO Audit s.r.o., BDO Czech Republic s.r.o., BDO Consulting s.r.o., BDO Legal s.r.o., advokátní kancelář a BDO ZNALEX, s.r.o. Společnost je součástí mezinárodní sítě BDO, která celosvětově tvoří jednu z největších sítí auditorských a poradenských skupin. Zaměstnává více jak 91 tisíc odborníků a působí ve 167 zemích, v nichž čítá více než 1 650 kanceláří.

Kontakt:
Jan Kuliš, EPIC Public relations,
E-mail: jan.kulis@epicpr.cz
Tel.: +420 731 920 874,
Web: www.epicpr.cz