TOMÁŠ ZÍTKO 27. 06. 2024 06:30

NIS2 přináší větší změny než GDPR. České firmy na něj ale nejsou připravené

Jaká nová pravidla směrnice NIS2 přináší, koho se týkají a jak se na ně připravit? Zeptali jsme se Tomáše Mauxe, experta na IT právo z Deloitte Legal.

ILUSTRACE: WIRED.CZ

Evropa se kyberneticky obrňuje před hrozbami z Ruska a Číny. Kvůli novým pravidlům směrnice NIS2 (Network and Information Security Directive 2) bude muset svá data a informační systémy začít lépe hlídat až 10 tisíc českých firem. Úroveň připravenosti je ale mezi nimi zatím velmi nízká. Podle nového průzkumu aliance NIS2READY 72 procent firem s přípravami ještě nezačalo, 26 procent respondentů pak uvedlo, že o nových pravidlech nic neví.

Za jejich porušení přitom mohou hrozit až stamilionové pokuty. Jaké změny tedy NIS2 přináší, koho se týká a kdy by mohl být schválen nový kyberbezpečnostní zákon, který evropské nařízení překlopí do českého práva?

„Evropská směrnice NIS2 představuje jednu z nejočekávanějších regulací letošního roku a je označována za regulaci co do rozsahu a dopadu větší než nařízení GDPR. Obdobně jako musely firmy implementovat mechanismy na ochranu osobních údajů, budou muset vybrané české společnosti poskytující regulované služby adresovat zcela novou oblast – kybernetickou bezpečnost," vysvětluje pro WIRED.CZ Tomáš Maux, expert na duševní vlastnictví, ochranu dat a právo informačních technologií v Deloitte Legal.

Jaké hlavní změny a povinnosti NIS2 přináší pro české firmy?

Především budou muset implementovat technická a organizační opatření, aby lépe řídily rizika spojená se svými sítěmi a informačními systémy. Mezi významnými povinnostmi je tu například povinnost rychleji a přesněji hlásit kybernetické incidenty příslušným orgánům, což je klíčové pro zajištění rychlé a koordinované reakce na případné hrozby. Směrnice také klade velký důraz na bezpečnost dodavatelských řetězců, kdy firmy budou muset zajistit, že i jejich dodavatelé dodržují vysoké standardy kybernetické bezpečnosti, což je zejména v poslední době tématem mnoha odborných diskusí.

„Podle odhadů NÚKIB se směrnice může dotknout zhruba 6 000 českých firem. Nicméně existují i další odhady, které naznačují, že počet firem může dosáhnout až 10 tisíc. "

Kromě toho budou firmy povinny provádět pravidelné audity a hodnocení bezpečnostních opatření, aby identifikovaly potenciální slabiny a mohly včas přijmout nápravná opatření. Dál je nutné zajistit školení zaměstnanců, aby byli dostatečně informováni a připraveni na případné kybernetické útoky. Směrnice také vyžaduje, aby firmy vypracovaly plány pro reakci na incidenty a zotavení po útoku, čímž se zvýší jejich odolnost a schopnost rychle obnovit činnost po jakémkoli narušení. To jsou však pouze vybrané zásadní povinnosti a směrnice NIS2 uvádí i mnohé další.

Kdy můžeme očekávat, že nová pravidla začnou platit?

Transpoziční lhůta dle směrnice NIS2 požaduje účinnost nového zákona k 18. říjnu letošního roku. Současný návrh zákona o kybernetické bezpečnosti z dílny Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) však dosud nevstoupil do schvalovacího procesu v Parlamentu. Poslední vývoj nastal dne 14. června, kdy legislativní rada doporučila návrh zákona vládě ke schválení.

Pokud k takovému schválení dojde, návrh zákona bude čekat standardní legislativní proces v Poslanecké sněmovně a v Senátu. Ačkoliv bylo původně v plánu návrh zákona schválit ještě v roce 2024 s účinností od 1. 1. 2025, už nyní lze předpokládat, že ani tento termín nebude možné z procesních důvodů stihnout. Realisticky lze odhadovat, že návrh zákona bude schválen v průběhu roku 2025 s účinností buď koncem toho roku, nebo od 1. 1. 2026.

Jak by se firmy měly na přijetí NIS2 připravit? Co jsou hlavní kroky, které by měly provést?

Společnosti by se měly zejména zaměřit na zodpovězení otázky, zda naplňují veškerá kritéria pro to, aby se na ně směrnice NIS2 nebo následně přijatý zákon o kybernetické bezpečnosti vůbec vztahoval. V obecné rovině lze říct, že společnost musí naplňovat současně dvě podmínky:

a) Je středním nebo velkým podnikem, tedy zaměstnává 50 a víc zaměstnanců, nebo dosahuje ročního obratu či bilanční sumy roční rozvahy alespoň 10 milionů eur (zhruba 250 milionů korun).

b) Poskytuje alespoň jednu službu uvedenou v přílohách směrnice NIS2.

Na závěr si pak firmy vyhodnotí dle kritérií, zda spadá do režimu vyšších, nebo nižších povinností. Neměly by proto s těmito procesy čekat, a to i s ohledem na případné nutné plánování rozpočtů na následující roky.

„V případě porušení vyšších, závažnějších povinností jsou pokuty až 250 milionů korun nebo dvě procenta z čistého celosvětového ročního obratu."

Kolika firem v Česku se NIS2 dotkne?

Podle odhadů NÚKIB se směrnice může dotknout zhruba šesti tisíc českých firem. Tento odhad zahrnuje subjekty, které spadají do klíčových odvětví a mají zásadní význam pro fungování společnosti a ekonomiky. Směrnice NIS2 se týká široké škály subjektů napříč různými sektory. V zásadě se zaměřuje na organizace, které jsou klíčové pro ekonomiku a společnost. To zahrnuje veřejnou správu, digitální infrastrukturu, energetiku, dopravu, bankovnictví, zdravotnictví a mnoho dalších sektorů.

Nicméně existují i další odhady, které naznačují, že počet firem může dosáhnout až 10 tisíc. Tento vyšší odhad bere v úvahu nejen hlavní subjekty, ale i jejich dodavatelské řetězce a další propojené organizace, které mohou být rovněž zranitelné vůči kybernetickým hrozbám, a proto by měly splňovat nové bezpečnostní požadavky. Je tedy možné, že skutečný počet firem, které budou muset zavést opatření podle NIS2, bude někde mezi těmito dvěma odhady. Bez ohledu na přesný počet je jasné, že směrnice bude mít široký dopad a mnoho českých firem bude muset zvýšit své úsilí v oblasti kybernetické bezpečnosti.

Jaké sankce budou firmám hrozit při nedodržení nových pravidel?

V případě porušení vyšších, závažnějších povinností jsou pokuty až 250 milionů korun nebo dvě procenta z čistého celosvětového ročního obratu. U nižších, méně závažných povinností jsou pokuty až 175 milionů korun nebo 1,4 procenta z čistého celosvětového ročního obratu. Kromě těchto pokut existují i další sankce, jako například pozastavení platnosti certifikace, pozastavení výkonu řídící funkce a udělování pořádkových nebo donucovacích pokut.

Jakou finanční zátěž pro firmy bude příprava na NIS2 představovat?

Náklady se mohou lišit v závislosti na velikosti firmy, komplexitě jejích systémů a aktuálním stavu její kybernetické bezpečnosti. Menší firmy budou zcela jistě čelit jiným nákladovým výzvám než velké korporace, které mají složitější infrastruktury a víc dat k ochraně. Kdo však věnoval čas a prostředky ochraně dat a kyberbezpečnosti doposud a dobrovolně, jeho náklady budou významně nižší.

Tomáš Zítko
Autor je redaktor WIRED. O dění na technologické scéně píše z byznysového hlediska, zejména se zaměřením na big tech firmy, sociální sítě, ale také domácí startupovou a e-commerce scénu. V minulosti působil v redakci zpravodajského serveru iHned.cz a v ekonomickém týmu Hospodářských novin. Vystudoval žurnalistiku na Univerzitě Karlově.