

Jak směrnice NIS2 ovlivní možnost používat druhotný software?

25.2.2025 - | PROTEXT

NIS2 - koho se to týká?

Nová legislativa se dotýká desítek tisíc společností v celé Evropské unii a přináší významné změny ve způsobu řízení kybernetické bezpečnosti ve veřejném i soukromém sektoru. Na rozdíl od své předchůdkyně, směrnice NIS, se dotýká mimo jiné veřejné správy, potravinářského průmyslu nebo nakládání s odpady.

Směrnice definuje dva typy subjektů:

Za podstatné subjekty a významné subjekty lze obecně považovat subjekty z odvětví uvedených v příloze I. a II. směrnice, které jsou minimálně středním podnikem (zaměstnávají minimálně 50 osob nebo jejichž roční obrát přesahuje 10 mil. EUR). Rovněž jsou zahrnuty další entity definované směrnicí NIS2, např. subjekty veřejné správy, subjekty označené jako kritické subjekty podle směrnice (EU) 2022/2557, poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací, kvalifikovaní poskytovatelé důvěryhodných služeb a registry doménových jmen nejvyšší úrovně a také poskytovatelé služeb DNS bez ohledu na jejich velikost. Na základě vnitrostátních právních předpisů mohou být zahrnuty i další subjekty. Směrnice však obsahuje několik výjimek. Nicméně do 17. dubna 2025 musí všechny členské státy vytvořit seznamy výše zmíněných subjektů, na které se budou nové předpisy vztahovat.

Vítaným pomocníkem, jak ověřit, zda bude mít na konkrétní společnost směrnice NIS2 dopad, může být web <https://portal.nukib.gov.cz/>. Tyto stránky provozuje Národního úřadu pro kybernetickou bezpečnost a informace, který je v ČR odpovědný za transpozici NIS2 do české legislativy. Na webu najdete nejen informace o aktuálním stavu implementace směrnice, ale také „kalkulačku“, která vám pomůže zjistit, zda se na vás NIS2 bude vztahovat.

Při řešení kybernetické bezpečnosti jde o implementaci systému řízení kybernetické bezpečnosti a vždy byste měli mít na paměti:

NIS2 vs. druhotný software

Ve své podstatě NIS2 neomezuje využívání druhotného softwaru, pokud jsou splněny parametry, které vyžaduje legislativa v této oblasti. Při výběru druhotného softwaru, kterým lze dosáhnout optimalizaci nákladů až do výše 70 procent ceny ve srovnání s nákupem softwaru přímo od výrobce, je ovšem třeba mít na paměti několik aspektů kybernetické bezpečnosti.

„Snažte se používat software, jehož životní cyklus produktu neskončil. To znamená, že pro takový produkt výrobce stále poskytuje nejnovější aktualizace ovlivňující mimo jiné vylepšenou kybernetickou bezpečnost. Tento cyklus někdy trvá přes deset let, ale vždy se vyplatí požádat softwarového brokera, jako je Forscope, o podrobnosti a odbornou pomoc. Ideální je, pokud vybraný broker nabízí rozšířenou škálu podpory, včetně technických, licenčních, compliance a právních služeb. Důvěryhodný broker by tohle měl být schopen nabídnout,“ doporučuje **Michal Baudyš, Public Sector Strategy Leader pro trhy v EU společnosti Forscope.**

Zde si připomeňme, že životní cyklus softwaru se obvykle skládá ze čtyř fází:

Alternativa k fázi tři a čtyři by mohla zahrnovat použití vyhrazených řešení ke zvýšení kybernetické bezpečnosti softwaru, který již výrobce nepodporuje. Tato řešení mohou také doporučit a poskytovat softwaroví brokeri.

Správci firemní IT infrastruktury by proto neměli zapomínat na pravidelnou instalaci záplat a aktualizací, které mohou pomoci zabránit tomu, aby byly systémy vystaveny útokům.

Kromě toho se vždy ujistěte, že používáte ověřený software od důvěryhodného brokera. Jeho výběr je zásadní, protože na trhu existují podvodné subjekty, které nabízejí například pouze produktové klíče bez řádné dokumentace. Případný nákup nelegálního software, byť v dobré víře, zvyšuje riziko soudních sporů, odpovědnost za škody za porušení práv duševního vlastnictví a navyšuje riziko instalace škodlivého softwaru v případě instalace z neznámých instalačních souborů.

<https://www.ceskenoviny.cz/tiskove/zpravy/jak-smernice-nis2-ovlivni-moznost-pouzivat-druhotny-software/2638972>