**Jak směrnice NIS2 ovlivní možnost používat**

**druhotný software?**

**V prosinci 2022 byla Evropskou unií schválena směrnice NIS2 (Network and Information System Directive 2), která stanovuje pravidla a požadavky na kybernetickou bezpečnost ICT systémů i sítí. NIS2 měly jednotlivé země EU implementovat do svých právních řádů do 18. října 2024. V praxi se tak ale dosud v řadě zemí nestalo, včetně ČR, kde se počítá se zavedením v polovině roku. Dotknou se nová, přísnější pravidla možnosti využívat druhotný software?**

**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:

* Základní subjekty s nejširším rozsahem odpovědností.
* Důležité subjekty, které musí splňovat méně přísné požadavky, ale stále podléhají regulaci.

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 obrat 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:

* stupeň rizika,
* míru hrozících následků,
* rozpočet, který je k dispozici,
* přiměřenost.

**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:

* 1. fáze – plná podpora. Softwarové aktualizace pokrývající jak bezpečnostní problémy, tak další oblasti jako je vylepšování funkcionality apod. a umožňuje vznést na výrobce požadavky na úpravy a funkce.
* 2. fáze – rozšířená podpora. V této fázi již není možné žádat o změny produktu nebo funkčnosti, protože jsou již poskytovány pouze aktualizace kybernetické bezpečnosti. Stejný zůstává přístup k podpoře.
* 3. fáze – po podpoře. Stále je možné využívat aktualizace z oblasti kybernetické bezpečnosti, ale pouze za příplatek. Zároveň jde nejzazší okamžik, kdy je nutné se poohlédnout po novějším softwaru.
* 4. fáze – software již není podporován.

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 brokeři.

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.

**O Forscope**

Forscope, největší softwarový broker ve střední a východní Evropě, nabízí plně licencovaná softwarová řešení prostřednictvím inovativního, nákladově efektivního modelu akvizice společnostem všech velikostí i veřejným institucím. Kromě toho společnost dodává komplexní balíček služeb včetně technické podpory, licenčního a právního poradenství. Forscope se sídlem v České republice působí v dalších 9 zemích střední a východní Evropy. Společnost je certifikovaným partnerem společnosti Microsoft a je držitelem certifikací ISO 9001:2015 a ISO 27001.

Pro více informací, navštivte: [Web](http://www.forscope.eu/) | [LinkedIn](https://www.linkedin.com/company/forscope/posts/?feedView=all) | [Facebook](https://www.facebook.com/Forscope/)

**Kontakt pro média**

Petra Losertová / Phoenix Communication, a.s.

E-mail: [petra@phoenixcom.cz](mailto:petra@phoenixcom.cz)

Tel: +420 728 162 140