Parlament České republiky

POSLANECKÁ SNĚMOVNA

2022

9. volební období

106.

USNESENÍ

výboru pro evropské záležitosti
ze 17. schůze
ze dne 2. listopadu 2022

k návrhu nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020 /kód Rady 12429/22, KOM(2022) 454 v konečném znění/

Výbor pro evropské záležitosti Poslanecké sněmovny Parlamentu ČR po vyslechnutí informace ředitele odboru kybernetických bezpečnostních politik Národního úřadu pro kybernetickou a informační bezpečnost Petra Novotného, po vyslechnutí zpravodajské zprávy posl. Jaroslava Bžocha a po rozpravě

1. **p r o j e d n a l** výše uvedený dokument;
2. **p o d p o r u j e ,** iniciativu Evropské komise v oblasti kybernetické bezpečnosti;
3. **b e r e n a v ě d o m í ,** rámcovou pozici vlády k tomuto dokumentu;
4. **z d ů r a z ň u j e ,** že pravidla a povinnosti vyplývající z nařízení, musí být specifikovány tak, aby neohrozily konkurenceschopnost firem z EU vůči firmám ze třetích zemí, čímž by se zhoršila i sama kybernetická bezpečnost;
5. **p o v ě ř u j e ,** předsedu výboru pro evropské záležitosti, aby v rámci politického dialogu postoupil toto usnesení předsedkyni Evropské komise.

Martin Exner v. r.
ověřovatel

Jaroslav Bžoch v. r.
zpravodaj

Ondřej Benešík v. r.
předseda

Příloha k usnesení č. 106

POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY
PARLAMENTNÍ INSTITUT
DOKUMENTY EU

Požadavky na kybernetickou bezpečnost produktů s digitálními prvky

Informační podklad k návrhu nařízení o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky

NÁVRH NAŘÍZENÍ

Návrh nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020

COM(2022) 454 final, kód Rady 12429/22

Interinstitucionální spis 2022/0272/COD

- Právní základ:
  Článek 114 Smlouvy o fungování Evropské unie.
- Datum zaslání Poslanecké sněmovně prostřednictvím VEZ:
  16. 9. 2022
- Datum projednání ve VEZ:
  5. 10. 2022 (1. kolo)
- Procedura:
  Řádný legislativní postup.
- Předběžné stanovisko vlády (dle § 109a odst. 1 jednacího řádu PS):
  Datované dnem 26. října 2022.
- Hodnocení z hlediska principu subsidiarity:
  Návrh je v souladu s principem subsidiarity.

- **Odůvodnění a předmět:**

Návrh nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020 (dále jen „návrh nařízení“ nebo „nařízení“) zavádí **nová společná pravidla** ve vztahu ke kybernetické bezpečnosti **produktů s digitálními prvky** (hardware i software pro vzdálené zpracování dat).

Cílem návrhu nařízení je řešit existující problémy související s nízkou úrovní kybernetické bezpečnosti produktů s digitálními prvky a nedostatečnou informovaností konečných uživatelů o kybernetických rizicích těchto produktů.

Návrh nařízení stanovuje, že produkty s digitálními prvky lze **uvádět na trh** pouze v případě, že budou splňovat **konkrétní základní požadavky na kybernetickou bezpečnost**, a to s ohledem na **dobu životního cyklu těchto produktů**. V této souvislosti se stanovují základní požadavky a ukládají povinnosti výrobcům, distributorům a dovozcům v návaznosti na jejich úlohu v dodavatelském řetězci.

Výrobcům se ukládá povinnost **zajistit soulad produktů s digitálními prvky**, jež jsou dodávány na trh EU, **s bezpečnostními požadavky**, a to od jejich návrhu a vývoje až po jejich výrobu, postupovat přitom s náležitou péčí, pokud jde o bezpečnostní aspekty, a poskytovat bezpečnostní podporu a aktualizace softwaru pro opravy odhalených zranitelností.

Ve vztahu ke spotřebitelům jsou výrobci povinni dále zajistit jejich **dostatečnou informovanost o kybernetické bezpečnosti produktů**, které kupují a používají.

Kybernetická bezpečnost představuje jednu z hlavních priorit Komise a je základním kamenem digitální Evropy. Nárůst kybernetických útoků a silný přeshraniční rozměr kybernetické bezpečnosti vyžaduje podle Evropské komise přijetí společných pravidel na unijní úrovni.

Návrh nařízení navazuje na novou strategii kybernetické bezpečnosti EU, která byla představena v prosinci 2020 Evropskou komisí a Evropskou službou pro vnější činnost, a závěry Rady k této strategii z března 2021. Cílem této strategie je posílení odolnosti Evropy vůči kybernetickým hrozbám a zajištění využívání důvěryhodných a spolehlivých služeb a digitálních nástrojů.

V současné době platí pro tuto oblast několik právních předpisů EU, které však řeší jen některé aspekty spojené s kybernetickou bezpečností hmotných digitálních výrobků a případně softwaru zabudovaného do těchto výrobků. Navíc na vnitrostátní úrovni jsou členskými státy přijímána opatření vyžadující zvýšení kybernetické bezpečnosti. To může vést ke zvýšení právní nejistoty a zatížení povinných subjektů. Předpokládá se, že se nařízení pravděpodobně stane mezinárodně uznávaným referenčním bodem nad rámec vnitřního trhu EU, neboť touto oblastí se státy na mezinárodní scéně teprve začínají zabývat. To přinese výhodu pro EU na světových trzích.

Nařízení doplní existující rámec EU pro kybernetickou bezpečnost, tj. směrnici o bezpečnosti sítí a informací, směrnici o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (směrnice NIS 2), která je ve fázi projednávání v Radě a Evropském parlamentu, a akt EU o kybernetické bezpečnosti.

- Obsah a dopad:

Návrh nařízení stanoví:

a) pravidla pro **uvádění produktů s digitálními prvky na trh**, aby byla zajištěna kybernetická bezpečnost těchto produktů;

b) **základní požadavky** na návrh, vývoj a výrobu produktů s digitálními prvky a **povinnosti hospodářských subjektů** ve vztahu k těmto produktům s ohledem na kybernetickou bezpečnost;

c) základní požadavky na **procesy řešení zranitelnosti** zavedené výrobci k zajištění kybernetické bezpečnosti produktů s digitálními prvky během celého životního cyklu a povinnosti hospodářských subjektů ve vztahu k těmto procesům a

d) pravidla pro **dozor nad trhem** a prosazování výše uvedených pravidel a požadavků.

Nařízení se vztahuje na všechny **produkty**, které jsou přímo nebo nepřímo **připojeny k jinému zařízení nebo síti**. Předmětem nařízení nejsou zdravotnické prostředky, výrobky pro letecký průmysl nebo automobily, pro které jsou již požadavky na kybernetickou bezpečnost stanoveny ve stávajících předpisech EU.

Návrh nařízení ukládá **povinnosti výrobcům, dovozcům a distributorům v souvislosti s uváděním produktů s digitálními prvky na trh**. Všechny produkty s digitálními prvky **mohou být uváděny na trh** pouze tehdy, pokud **splňují stanovené podmínky** (příloha I oddíl 1 návrhu nařízení) a pokud jsou řádně instalovány, udržovány a používány k určenému účelu nebo za podmínek, které lze rozumně předvídat, a postupy zavedené výrobcem splňují základní požadavky **ve vztahu k řešení zranitelností produktů s digitálními prvky** (příloha I oddíl 2 návrhu nařízení), např. povinnost identifikovat a dokumentovat zranitelnosti a součásti obsažené v produktu a povinnost bez zbytečného odkladu řešit a odstraňovat zranitelnosti, především prostřednictvím bezpečnostní aktualizace. Výrobce je povinen provést **analýzu rizik**, aby identifikoval požadavky v oblasti kybernetické bezpečnosti, které jeho produkt musí splňovat (příloha I oddíl 1 bod 3 nařízení). Při začleňování komponentů produktu pocházejících od třetích stran do produktů s digitálními prvky musí výrobce **postupovat s náležitou péčí** tak, aby tyto komponenty neohrozily bezpečnost tohoto produktu.

Povinnost výrobce **zajišťovat bezpečnost produktů** s digitálními prvky je stanovena na dobu pěti let nebo po dobu životnosti produktu, přičemž se počítá doba, která bude kratší. Výrobcům se dále ukládá **povinnost informovat** Agenturu Evropské unie pro kybernetickou bezpečnost (dále jen „ENISA“) do 24 hodin od okamžiku, kdy se dozví o aktivně zneužívaných zranitelnostech produktů s digitálními prvky či incidentech s dopadem na bezpečnost takových produktů.

Výrobci jsou povinni podstoupit **proces posuzování shody produktu s digitálními prvky a řešení zranitelnosti**, aby prokázali, zda byly splněny požadavky týkající se produktu stanovené v příloze I návrhu nařízení. Pro účely posuzování shody jsou produkty rozčleněny na standardní a kritické produkty s digitálními prvky. Příkladem standardních produktů s digitálními prvky je software pro úpravu fotografií, zpracování textu, chytré reproduktory, pevné disky nebo hry. **Kritické produkty s digitálními prvky** jsou rozděleny do třídy I a třídy II (příloha III návrhu nařízení), což odráží jejich úroveň rizika kybernetické bezpečnosti, přičemž třída II představuje vyšší riziko. Za kritické produkty I. třídy jsou považovány např. správci hesel, síťová rozhraní nebo síťové brány, za kritické produkty II. třídy pak operační systémy, průmyslové firewally nebo procesory. Kritické produkty podléhají **přísnějším postupům posuzování shody**, kdy pro kategorii II. třídy nestačí sebehodnocení provedené výrobcem, ale je nezbytné posouzení shody třetí stranou. Po prokázání souladu produktu se stanovenými požadavky se vypracovává prohlášení o shodě s označením CE, které umožní jeho volný pohyb na vnitřním trhu. Komise je zmocněna k přijímání aktů v přenesené pravomoci za účelem doplnění tohoto nařízení stanovením **kategorií vysoce kritických produktů s digitálními prvky,** pro které musí výrobci získat evropský certifikát kybernetické bezpečnosti v rámci evropského systému certifikace kybernetické bezpečnosti, aby prokázali shodu se základními požadavky stanovenými v příloze I návrhu nařízení.

Nařízení také upravuje pravidla pro **předpoklad shody**, který se uplatní na produkty s digitálními prvky a postupy zavedené výrobcem, které budou odpovídat harmonizovaným normám, a na něž

byly zveřejněny odkazy v Úředním věstníku EU, dále na produkty a procesy, které budou ve shodě s obecnými specifikacemi podle čl. 19 nařízení, stejně jako na produkty, pro něž bylo vydáno prohlášení EU o shodě či certifikát dle evropských certifikačních schémat kybernetické bezpečnosti dle aktu EU o kybernetické bezpečnosti. Pokud harmonizované normy neexistují nebo jsou nedostatečné, pokud v postupu normalizace dochází ke zbytečným průtahům nebo pokud žádost Komise nebyla přijata evropskými normalizačními organizacemi, může Komise pomocí prováděcích aktů přijmout obecné specifikace. Komise je oprávněna také upřesnit, zda certifikát kybernetické bezpečnosti vydaný v rámci evropského systému certifikace kybernetické bezpečnosti odstraňuje povinnost výrobců provést posouzení shody třetí stranou, jak je stanoveno v nařízení.

Výrobci mají rovněž povinnost zajistit, aby k produktům s digitálními prvky **byly přiloženy informace a pokyny** stanovené v příloze II, a to v elektronické nebo fyzické podobě. Tyto informace a pokyny musí být v jazyce, který je pro uživatele snadno srozumitelný. Musí být jasné, srozumitelné, pochopitelné a čitelné. Musí umožňovat bezpečnou instalaci, provoz a používání produktů s digitálními prvky. Příloha II stanovuje minimální informace a pokyny, které musí být uživatelům předány společně se samotným produktem, např. jméno, registrované obchodní jméno či značku výrobce společně s kontaktní a emailovou adresou; kontaktní místo, kde lze oznámit nebo získat informace o zranitelnostech daného produktu; zamýšlené použití, včetně bezpečnostního prostředí poskytovaného výrobcem, jakož i základní funkce produktu a informace o jeho bezpečnostních vlastnostech.

Návrh nařízení stanoví požadavky na **vnitrostátní orgány**, které jsou odpovědné za orgány posuzování shody (oznámené subjekty). Návrh ponechává konečnou odpovědnost za jmenování a kontrolu oznámených subjektů členským státům. Členským státům se ukládá povinnost určit oznamující orgán odpovědný za vytvoření a provádění nezbytných postupů pro posuzování a oznamování subjektů posuzování shody a za kontrolu oznámených subjektů. Členské státy mají dále povinnost oznámit Komisi a ostatním členským státům subjekty, které budou oprávněny provádět úkoly spojené s posuzováním v souladu s nařízením.

Členské státy jsou povinny jmenovat orgány dozoru nad trhem, které jsou odpovědné za vymáhání povinností vyplývajících z nařízení. Nařízení stanovuje povinnosti a pravomoci orgánů dozoru nad trhem. Například v případě neshody produktů s požadavky stanovenými v nařízení mají orgány dozoru nad trhem oprávnění od příslušných subjektů požadovat, aby nesoulad ukončily a odstranily riziko, zakázaly nebo omezily dodávání produktu na trh nebo nařídily stažení produktu. Každý z těchto orgánů dozoru nad trhem je oprávněn pokutovat subjekty, které nedodržují stanovená pravidla. Nařízení stanoví maximální úrovně správních pokut, které by měly být stanoveny ve vnitrostátních právních předpisech za nedodržení požadavků stanovených nařízením.

- Stanovisko vlády ČR:

  Vláda vítá ambici Evropské komise zajistit kybernetickou bezpečnost digitálních produktů na vnitřním trhu prostřednictvím horizontálních požadavků, které mohou výrazně přispět k ochraně a informovanosti uživatelů. Je však nezbytné, aby opatření a nástroje přijaté k dosažení těchto cílů byly proporcionální a umožnily dotčeným soukromým společnostem zůstat konkurenceschopnými a inovativními. Implementace nové regulace s sebou přináší nejen potřebu alokovat nové kapacity, ale i ekonomické zdroje. Finanční a administrativní zátěž bude zřejmě výrazně dopadat zejména na malé a střední podniky, proto ČR bude usilovat o to, aby jednotlivá opatření zohledňovala povahu a specifika jejich fungování tak, aby nebyla ohrožena jejich činnost.

  ČR zvláště vítá aspekty nařízení, jejichž aplikace může vést ke zvýšení bezpečnosti dodavatelského řetězce produktů s digitálními prvky, např. povinnost hlášení incidentů majících dopad na bezpečnost

produktu, zahrnutí softwarových a hardwarových komponentů do působnosti nařízení a povinnost náležité péče výrobce. Tyto povinnosti jsou však pro výrobce náročné a nákladné, a proto vláda navrhuje jejich usnadnění, např. zavedením jednotného formuláře pro hlášení a vyjasněním možných způsobů plnění povinnosti náležité péče.

ČR považuje za stěžejní, aby byla jasně stanovena provázanost nařízení s další legislativou v oblasti kybernetické bezpečnosti, jmenovitě se směrnicí NIS 2, aktem o kybernetické bezpečnosti, návrhem aktu o umělé inteligenci a dalšími legislativními akty upravujícími bezpečnost výrobků uváděných na vnitřní trh. ČR se bude zasazovat o to, aby nedocházelo k nežádoucím překryvům a rozporům nařízení a související legislativy.

- Předpokládaný harmonogram projednávání v orgánech EU:
  V Evropském parlamentu je výborem odpovědným za projednání návrhu výbor pro průmysl, výzkum a energetiku (ITRE). O stanovisko k návrhům byly také požádány další výbory, konkrétně výbor pro občanské svobody, spravedlnost a vnitřní věci (LIBE) a výbor pro vnitřní trh a ochranu spotřebitelů (IMCO).

Ve spolupráci se zpravodajem výboru pro evropské záležitosti Jaroslavem Bžochem zpracovala Mgr. Andrea Pokorná, odborná konzultantka Parlamentního institutu Kanceláře PS PČR.