8. 11. 2023

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Evropa brání svou digitální budoucnost: Akt o kybernetické odolnosti

V posledních letech se EU zaměřuje na podporu digitalizace a digitální transformace ve společnosti, což je patrné z mnoha nových právních předpisů. Digitalizace však přináší i řadu výzev a jednou z nich je i zvýšené riziko kybernetických útoků, které mohou ohrozit bezpečnost našich dat. Proto je jedním z nejnovějších počinů v oblasti kyberbezpečnosti EU akt o kybernetické odolnosti, který v létě schválil klíčový výbor Evropského parlamentu.

Nařízení si klade za cíl vyplnit prázdná místa v existujících právních předpisech a zaměřuje se především na produkty, které jsou přímo nebo nepřímo připojeny k jinému zařízení nebo síti a pro které doposud neexistuje žádná zvláštní právní úprava.

Akt zavádí plošný přístup k výrobcům a vývojářům, kteří nesou největší odpovědnost za technologické zabezpečení produktů. Nařízení ve svém návrhu a důvodové zprávě zmiňuje, že produkty uváděné na trh trpí nejčastěji dvěma hlavními problémy:

- nízkou kybernetickou bezpečností, která se projevuje v rozšířené zranitelnosti a nedostatečnému poskytování bezpečnostních aktualizací, a
- nedostatečnému povědomí uživatelů o kybernetické bezpečnosti projevující se tím, že si uživatelé nevybírají dostatečně bezpečné produkty anebo je nepoužívají dostatečně obezřetně ve vztahu k těmto rizikům (ať už se jedná o hardwarové nebo softwarové produkty).

Tato situace pak může potenciálně ohrožovat jednotlivé organizace anebo celé dodavatelské řetězce a mít tak závažné dopady na hospodářské a sociální aktivity.

Akt o kybernetické odolnosti ukládá (za účelem zmírnění popsaných rizik) na výrobce novou řadu povinností. Mezi jednu z nejvýznamnějších patří povinnost uvádět na trh pouze ty produkty, které splňují základní bezpečnostní požadavky stanovené přílohou tohoto aktu v poměrně obecně rovině.

Výrobci budou muset provést posouzení rizik týkajících se kybernetické bezpečnosti ve svých produktech s digitálními prvky a vycházet z těchto závěrů při plánování vývoje a výroby svých produktů tak, aby bylo minimalizováno riziko kybernetických útoků, bezpečnostních incidentů a jejich následků. Toto posouzení budou muset mít výrobci i vývojáři řádně zdokumentováno a průběžně jej budou muset aktualizovat po celou dobu provozu jejich produktu.

Různé povinnosti pro různé výrobky

Návrh nařízení navíc rozlišuje mezi různými kategoriemi výrobků. Je pochopitelné, že některé výrobky s digitálními prvky by měly podléhat přísnějším postupům posuzování s ohledem na riziko vzniku bezpečnostního/kybernetického incidentu.

Nařízení tak rozděluje produkty na **výrobky třídy 1** (např. software pro vydávání digitálních certifikátů anebo routery či modemy určené k připojení k internetu), jež si budou moci jejich výrobci certifikovat sami, a **výrobky třídy 2** (kritičtější), které budou vyžadovat posouzení kybernetických

rizik nezávislým auditorem (zde se jedná např. o produkty podporující funkce VPN anebo o firewally či jiné systémy detekce anebo prevence narušení systémů).

Za nedodržení základních požadavků na kybernetickou bezpečnost stanovených v příloze aktu o kybernetické odolností se budou ukládat pokuty až do výše 15 000 000 EUR anebo až do výše 2,5 % celkového celosvětového ročního obratu výrobce či vývojáře.

Kritika open-source projektů či návrhy na doporučení od největších hráčů

K novému právnímu předpisu se již strhla rozsáhlá debata týkající se jeho vyváženosti a nejasností ohledně definic. Zástupci několika open source projektů sepsali společný otevřený dopis, v němž varují před novou legislativou, která může zkomplikovat vývoj softwaru s otevřeným zdrojovým kódem.

Akt o kybernetické odolnosti sice vylučuje ze své působnosti projekty a software vyvíjený mimo rámec obchodní činnosti, avšak opomíjí či nezohledňuje skutečnost, že některé open source projekty jsou finančně podporovány pro svůj chod anebo účtují poplatky pouze za servisní služby (nikoliv za vývoj a distribuci open source software). Tyto otázky by tedy měly být evropskými legislativci zváženy.

K návrhu se vedle těchto iniciativ vyjádřily i přední technologické společnosti, jmenovitě Microsoft, který ve svém vyjádření dává zástupcům v Evropské unii několik podrobných doporučení, které by pomohly:

- zajistit větší srozumitelnost a předvídatelnost nařízení,
- zajistit připravenost a kapacitu dotčených stran k provádění nařízení, a
- sladit povinnosti uvedené v nařízení se stávajícími mezinárodními bezpečnostními standardy a osvědčenými postupy tak, aby se zabránilo roztříštěnosti a oslabení bezpečnosti uživatelů na celém světě.

Jak se připravit?

Poté, co bude schválen návrh nařízení, budou mít výrobci dva roky na splnění jejich povinností. Úplné dodržování těchto předpisů však pravděpodobně nebude s ohledem na aktuální stav legislativního procesu povinné dříve než v roce 2025.

Je tedy nutné se začít připravovat již nyní? Na tuto otázku není jednoduché odpovědět, bude však zajímavé sledovat, jakých případných změn nařízení dozná po následující diskuzi v trialogu národních vlád s Evropskou komisí a Evropským parlamentem.

Akt o kybernetické odolnosti má potenciál být stejně komplexní a revoluční ve změně způsobu, jakým výrobci a poskytovatelé softwaru pro internet věcí (IoT) řídí zabezpečení svých produktů, podobně jako mělo například GDPR vliv na podnikatele a na jejich způsoby, jakým nakládají s osobními údaji.

Mgr. Pavel Amler,
senior advokát

Mgr. Tomáš Lupač,
koncipient

HAVEL & PARTNERS
ÚSPĚCH SPOJUJE

HAVEL & PARTNERS s.r.o., advokátní kancelář

Florentinum, recepce A
Na Florenci 2116/15
110 00 Praha 1

Tel.: +420 255 000 111
Fax: +420 255 000 110
e-mail: office@havelpartners.cz

Další články:

- Evropská unie mění pravidla plateb: více odpovědnosti, intenzivnější zpracování dat, více kontrol
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Novinky z české a evropské regulace finančních institucí za měsíc květen 2026
- Sport versus EU – aktuální sportovní kauzy rozhodované Soudním dvorem EU
- Postavení finančního arbitra v kontextu nařízení Brusel I bis - Funkční pojetí „soudu“, osvědčení podle čl. 53 a možnost výkonu nálezu v jiných členských státech EU

- ESG Simple jako praktická opora pro ESG reporting malých a středních podniků
- Novinky z české a evropské regulace finančních institucí za měsíc duben 2026
- Dvě kiwi denně: EU schválila první zdravotní tvrzení pro čerstvé ovoce
- Digital Omnibus: Revoluce v datech, nebo jen nová zátěž pro podnikatele?
- Nová pravidla pro ground handling v EU a jejich dopady na letecký sektor
- Novinky z české a evropské regulace finančních institucí za měsíc březen 2026