

Skrytá rizika nákupu softwaru a jak se jim vyhnout

24.7.2025 - | Phoenix Communication

Představa, že nový software je automaticky bezpečný, je mylná. Na trhu s novými licencemi se opakovaně objevují podvody, kdy bezohlední prodejci vydávají neplatné klíče za plnohodnotné licence. Využívají přitom složitosti licenčních modelů a neznalosti zákazníků. U druhotného softwaru je situace o něco odlišná - zde je klíčové ověřit řetězec vlastnictví licence, aby byla zajištěna její právní platnost. „Bez řádné dokumentace hrozí, že software nebude splňovat podmínky auditu,“ říká Jakub Šulák, zakladatel a CEO společnosti Forscope, která je jedničkou na trhu se sekundárním softwarem ve střední a východní Evropě a poskytla své služby více než 15 000 firmám či institucím.

Dalším problémem je nesprávné licencování, zejména u komplexních systémů, jako jsou serverová prostředí nebo ERP. Dodavatelé někdy upravují nabídky, aby vyhověly rozpočtu zákazníka, což může vést k porušení licenčních podmínek. Například připojení více uživatelů pod jednou licencí, ačkoliv se může zdát jako efektivní řešení, často odporuje pravidlům výrobce. *„Taková praxe ohrožuje nejen právní platnost licence, ale může také narušit spolehlivost systému a jeho auditní stopy, což může mít vážné důsledky pro bezpečnost dat,“* vysvětluje Jakub Šulák.

Doporučení pro bezpečný nákup

Aby se organizace vyhnuly rizikům, měly by při nákupu softwaru dodržovat několik zásad:

Společnosti jako Forscope nabízejí transparentní procesy a podrobnou dokumentaci, která zaručuje soulad s právními předpisy. Jejich interní postupy jsou navrženy tak, aby klienti obdrželi software odolný vůči auditu, což je zvláště důležité pro velké organizace a veřejný sektor.

Výzvy veřejného sektoru

Veřejné instituce čelí přísnějším pravidlům zadávání zakázek, což omezuje jejich flexibilitu při výběru dodavatelů. Přesto mohou přijmout opatření, jako je požadavek na ověření referencí nebo pojištění dodavatele. *„Častou chybou je přílišná důvěra v elektronické dokumenty nebo notářsky ověřená prohlášení. Podle nařízení EU eIDAS je elektronický podpis definován široce a zahrnuje i prosté textové podpisy v e-mailech. Notářské ověření naopak není zárukou pravdivosti, protože podvodníci mohou snadno předložit nepravdivá prohlášení,“* varuje Jakub Šulák.

Další problematickou praxí je hodnocení nabídek pouze podle ceny bez důkladného prověření dokumentace. To vytváří prostor pro nekvalitní nebo nelegální nabídky, které nemusí splňovat požadavky na autorská práva v EU/EHP. *„Veřejní zadavatelé by měli klást důraz na ucelený řetězec důkazů o původu licence, podobně jako soudy, které nevyžadují každý důkaz v originále, ale hodnotí jejich konzistenci,“* zdůrazňuje Jakub Šulák.

Příležitosti druhotného trhu

Sekundární trh se softwarem nabízí organizacím významné úspory bez kompromisů v kvalitě, pokud je nákup proveden správně. *„Klíčem je spolupráce s důvěryhodnými dodavateli, jako je Forscope, kteří poskytují podrobnou dokumentaci a zajišťují soulad s právními předpisy. Zkušenosti kupující často využívají právní konzultace, aby ověřili, zda licence splňují podmínky, jako je řádné odinstalování a původ v EU/EHP,“* říká Jakub Šulák.

Rostoucí hrozby a řešení

S rostoucí cenou nelegálních softwarových nabídek se podvodníci snaží působit důvěryhodněji tím, že nabízejí software za ceny těsně pod tržní hodnotou. To zvyšuje riziko ztrát pro kupující i výrobce softwaru. Organizace by proto měly:

„Trh se softwarem je plný příležitostí, ale i rizik. Rozhodující je pečlivost při výběru partnera. Důvěryhodní dodavatelé nabízejí nejen atraktivní ceny, ale především transparentní procesy a právní jistotu,“ uzavírá Jakub Šulák.

<https://www.phoenixcom.cz/press/skryta-rizika-nakupu-software-a-jak-se-jim-vyhnout>