

Správa softwarových licencí | Behaviorální analytika |
Inovace podnikových úložišť | Správa podnikových dat | Průmyslové Wi-Fi

COMPUTERWORLD®

UCELENÝ INFORMAČNÍ ZDROJ PRO IT PROFESIONÁLY CENA 50 Kč/2,6 € | COMPUTERWORLD 11/2023 | ROČNÍK XXXIV | 31. 10.–29. 11. 2023

Pozor na umělou inteligenci

AI pomáhá v životě i v podnicích,
ale také podvodníkům.
Připravte se!



IT produkt
FINALISTÉ TŘETÍHO KOLA

Máte licence? A mohla bych je vidět? 2

Tisk, Computerworld (CZ), 31. 10. 2023

Máte licence? A mohla bych je vidět?

31. 10. 2023, Zdroj: **Computerworld (CZ)**, Strany: 32, 33, Vydavatel: **Internet Info DG, a.s.**, Autor: **Lenka Hanková**

Rubrika: **SERIÁL | IT A PRÁVO (42)**

Užívání nelegálních softwarů jak jednotlivci, tak společnostmi je stále realitou, i když doba, kdy jejich použití v podstatě nebylo možné zjistit, je dávno pryč.

Nejen velké technologické firmy, ale už i menší vývojáři si s pomocí nových technologií dokážou duševní vlastnictví pohlídat, resp. zjistit, zda jej někdo nepoužívá bez oprávnění, tedy licence. Proto by se softwarovým licencím měla ve firmách věnovat zvláštní pozornost (tzv. software asset management), neboť již nyní jsou softwary v mnoha z nich základním „výrobním“ prostředkem.

Z pohledu práva rozumíme licenci oprávnění k výkonu práva duševního vlastnictví v určitém rozsahu, který je zpravidla ujednáán v licenční smlouvě nebo licenčních podmínkách, příp. stanoven v zákoně. Práva a povinnosti stran licenční smlouvy jsou v českém právu upraveny v § 2358 a násl. občanského zákoníku (zákon č. 89/2012 Sb.) a práva samotného autora a následky jejich porušení navíc v autorském zákoně (zákon č. 121/2000 Sb.).

V určitých vlnách se společnosti i jednotlivci obracejí na právníky s tím, že obdrželi výzvy od výrobců softwarů či jejich právních zástupců, mediátorů a různých agentur, které tvrdí, že používají software nelegálně, a požadují uhrazení vysokých částek. V lepším případě nabízejí smírné řešení v podobě zakoupení legální verze softwaru, což i tak představuje výrazný zásah do firemního rozpočtu. U jednotlivců se potom může stát, že částku nebudou schopni uhradit vůbec.

Svoje nároky výrobci zpravidla opírají o data, která získali prostřednictvím speciálních sledovacích technologií (např. phone home technology). Pokud dojde k pozměnění softwaru (cracknutí) za účelem jeho použitelnosti i pro další uživatele, sledovací technologie se aktivuje a začne sbírat data jako např. MAC adresu počítače, doménové jméno, ze kterého se hlásí, datum a čas použití apod.

Takovou změnu softwaru a jeho použití bez řádné licence lze definovat jako porušení práv autora (resp. držitele příslušných majetkových práv). Pokud výrobce ve své výzvě či v další komunikaci uvede provozní data poskytnuté a jsou průkazná, může být situace pro podnikatele poměrně složitá, aby se z tvrzeného porušení licenčních práv vyvinil. Forma vyvinění, tj. prokázání řádné licence, závisí na konkrétním případě. K tomu, aby se výrobci dozvěděli o nelegálním softwaru, ovšem někdy stačí i prosté udání bývalým zaměstnancem, nespokojeným zákazníkem nebo dodavatelem, případně může jít i o nekalou praxi konkurence.

Jak se takový nelegální software může vůbec ve firmě objevit? Na úvod je třeba zmínit nejzávažnější variantu, tj. že byl software nainstalován a používán úmyslně s vědomím, že je nelegální. Podobně problematická je rovněž situace, kdy za nelegální verzi firma zaplatila pochybnému „distributorovi“ či poskytovateli tzv. druhotných licencí, které ne vždy splňují všechna kritéria legality.

Často se také stává, že firma si sice licenci legálně pořídila, ale nainstaluje software ve více počítačích, než má povoleno, nebo zapomene na odinstalování původní verze po zakoupení nové. A samozřejmě nemůžeme vynechat ani instalaci softwaru na firemní PC pracovníky bez vědomí zaměstnavatele, nebo případy, kdy si zaměstnanec či spolupracující dodavatel „ičař“ nainstaluje firemní software na soukromý počítač, z něhož se potom připojí k firemní síti. To vše lze podřadit pod porušení autorských práv, příp. porušení licenčních podmínek, byla-li licenční smlouva uzavřena.

Co v takových případech hrozí? Když zůstaneme v občanskoprávní sféře, držitelé práv k softwarům mají podle § 40 a násl. autorského zákona řadu možností, jak se bránit. Mohou soudně požadovat zákaz užívání takového softwaru, jeho stažení nebo zničení, sdělení údajů o způsobu a rozsahu neoprávněného užití a o původu softwaru či zveřejnění rozsudku. Dále mohou nárokovat přiměřené zadostiučinění (omluvu či peněžní náhradu), náhradu škody včetně ušlého zisku a bezdůvodného obohacení. Autorský zákon přitom výši bezdůvodného obohacení stanoví jako dvojnásobek odměny, která by byla za získání takové licence obvyklá v době neoprávněného užívání softwaru.

Pokud se výrobcem oslovená firma rozhodne na výzvy reagovat, nastává zpravidla kolotoč korespondence. V této fázi je nutné nepodléhat panice a zjistit, co vlastně softwarová společnost požaduje, jakou relevanci mají její důkazy, a prověřit její zastoupení (aby třeba nešlo o phishing). Ve většině případů se přitom strany nějakým způsobem dohodnou, případně výrobce ustoupí ze svého požadavku, zvláště pokud uzná, že by v dané situaci neměl dobrou důkazní pozici.

Někdy nicméně softwarový výrobce začne uplatňovat i právo na audit (kontrolu) všech zařízení firmy. Licenční či všeobecné obchodní podmínky softwarových firem toto právo ve většině případů skutečně obsahují. Otázkou ovšem je, zda při instalaci nelegálního softwaru byly takové licenční podmínky vůbec uzavřeny. Logicky nikoliv, neboť základním předmětem licenční smlouvy je právě udělení oprávnění (licence) poskytovatelem nabyvateli. S požadavkem na audit se proto většinou lze v praxi setkat např. u subjektů, které sice zakoupily legální licenci, ale použily ji na více počítačů, než jim podmínky povolovaly, nebo které zapomněly původní software s propadlou licencí odinstalovat.

V horším případě mohou být jak společnost (neboť i právnické osoby jsou podle českých právních předpisů trestně odpovědné), tak i jednotlivci vyšetřováni policií a souzeni v trestněprávním řízení pro porušení autorského práva. Podle § 270 trestního zákoníku (zákon č.

40/2009 Sb.) platí, že uvedený trestný čin spáchá ten, kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu.

Pokud by vznikla škoda velkého rozsahu (dosahující nejméně deseti milionů korun), hrozí trest odnětí svobody až na osm let. Nutno říci, že ke spáchání tohoto trestného činu je zapotřebí úmyslu. Pokud by došlo k porušení autorského práva z nedbalosti, bylo by možné potrestat viníka pouze za spáchání přestupku. V praxi jsou přitom zpravidla ukládány podmíněné tresty odnětí svobody, příp. další tresty jako zákaz činnosti, zabavení a propadnutí počítačové techniky.

Asi neprozradím nic nového, když uvedu, že prevence těchto komplikovaných situací v podobě efektivního software asset managementu je pro firmy zcela zásadní. Může jít například o: ■ přijetí interní dokumentace (např. směrnice), která zakazuje instalaci jakéhokoliv softwaru bez souhlasu zaměstnavatele, ■ pravidelná školení (nejen při náboru zaměstnance), ■ zavedení technických a organizačních opatření v souvislosti se zabráněním instalace softwaru bez souhlasu administrátora a pravidelné kontroly, ■ zavedení pouze kontrolované firemní výpočetní techniky (zákaz BYOD) či ■ prověření distributora (prodejce) licence, potažmo legálnosti licencí před zakoupením.

Sečteno a podtrženo: vždy platí zlaté heslo „důvěřuj, ale prověřuj“. Bez kontrolních mechanismů a pravidelných softwarových auditů firmy riskují. Pokud však zavedou dostatečná opatření, mají i dobrou šanci vyvinut se z případné žaloby za porušení autorského práva zaměstnancem.

Autorka je advokátka, **Rödl** & Partner, advokáti

Softwarovým licencím by se měla ve firmách věnovat zvláštní pozornost.

Pokud by vznikla škoda velkého rozsahu (dosahující nejméně deseti milionů korun), hrozí trest odnětí svobody až na osm let.

Autor: LENKA HANKOVÁ

Máte licence? A mohla bych je vidět?

LENKA HANKOVÁ

Užívání nelegálních softwarů jak jednotlivci, tak společnostmi je stále realitou, i když doba, kdy jejich použití v podstatě nebylo možné zjistit, je dávno pryč.

N ejen velké technologické firmy, ale už i menší vývojáři si s pomocí nových technologií dokážou duševní vlastnictví pohlídat, resp. zjistit, zda jej někdo nepoužívá bez oprávnění, tedy licence. Proto by se softwarovým licencím měla ve firmách věnovat zvláštní pozornost (tzv. software asset management), neboť již nyní jsou softwary v mnoha z nich základním „výrobním“ prostředkem.

Softwarovým licencím by se měla ve firmách věnovat zvláštní pozornost.

Z pohledu práva rozumíme licenci oprávnění k výkonu práva duševního vlastnictví v určitém rozsahu, který je zpravidla ujednán v licenční smlouvě nebo licenčních podmínkách, příp. stanoven v zákoně. Práva a povinnosti stran licenční smlouvy jsou v českém právu upraveny v § 2358 a násl. občanského zákoníku (zákon č. 89/2012 Sb.) a práva samotného autora a následky jejich porušení

navíc v autorském zákoně (zákon č. 121/2000 Sb.).

V určitých vlnách se společnosti i jednotlivci obracejí na právníky s tím, že obdrželi výzvy od výrobců softwarů či jejich právních zástupců, mediátorů a různých agentur, které tvrdí, že používají software nelegálně, a požadují uhrazení vysokých částek. V lepším případě nabízejí smírné řešení v podobě zakoupení legální verze softwaru, což i tak představuje výrazný zásah do firemního rozpočtu. U jednotlivců se potom může stát, že částku nebudou schopni uhradit vůbec.

Svoje nároky výrobci zpravidla opírají o data, která získali prostřednictvím speciálních sledovacích technologií (např. phone home technology). Pokud dojde k pozměnění softwaru (cracknutí) za účelem jeho použitelnosti i pro další uživatele, sledovací technologie se aktivuje a začne sbírat data jako např. MAC adresu počítače, doménové jméno, ze kterého se hlásí, datum a čas použití apod.



Takovou změnu softwaru a jeho použití bez řádné licence lze definovat jako porušení práv autora (resp. držitele příslušných majetkových práv). Pokud výrobce ve své výzvě či v další komunikaci uvedená provozní data poskytne a jsou průkazná, může být situace pro podnikatele poměrně složitá, aby se z tvrzeného porušení licenčních práv vyvinil. Forma vyvinění, tj. prokázání řádné licence, závisí na konkrétním případě. K tomu, aby se výrobci dozvěděli o nelegálním softwaru, ovšem někdy stačí i prosté udání bývalým zaměstnancem, nespokojeným zákazníkem nebo dodavatelem, případně může jít i o nekalou praktiku konkurence.

Jak se takový nelegální software může vůbec ve firmě objevit? Na úvod je třeba zmínit nejzávažnější variantu, tj. že byl software nainstalován a používán úmyslně s vědomím, že je nelegální. Podobně problematická je rovněž situace, kdy za nelegální verzi firma zaplatila pochybnému „distributorovi“ či poskytovateli tzv. druhotných licencí, které ne vždy splňují všechna kritéria legality.

Často se také stává, že firma si sice licenci legálně pořídila, ale nainstaluje software ve více kopiích, než má povoleno, nebo zapomene na odinstalování původní verze po zakoupení nové. A samozřejmě nemůžeme vynechat ani instalace softwaru na firemní PC pracovníky bez vědomí zaměstnavatele, nebo případy, kdy si zaměstnanec či spolupracující dodavatel „ičáři“ nainstaluje firemní software na soukromý počítač, z něhož se potom připojí k firemní síti. To vše lze podřadit pod porušení autorských práv, příp. porušení licenčních podmínek, byla-li licenční smlouva uzavřena.

Co v takových případech hrozí? Když zůstaneme v občanskoprávní sféře, držitel práv k softwarům mají podle § 40 a násl. autorského zákona řadu možností, jak se bránit. Mohou soudně požadovat zákaz užívání takového softwaru, jeho stažení nebo zničení, sdělení údajů o způsobu a rozsahu neoprávněného užití a o původu softwaru či zveřejnění rozsudku. Dále mohou nárokovat přiměřené zadostiučinění (omluvu či peněžní náhradu), náhradu škody včetně ušlého zisku a bezdůvodného obohacení. Autor-



ský zákon přitom výši bezdůvodného obohacení stanoví jako dvojnásobek odměny, která by byla za získání takové licence obvyklá v době neoprávněného užívání softwaru.

Pokud se výrobcem oslovená firma rozhodne na výzvy reagovat, nastává zpravidla kolotoč korespondence. V této fázi je nutné nepodléhat panice a zjistit, co vlastně softwarová společnost požaduje, jakou relevanci mají její důkazy, a prověřit její zastoupení (aby třeba nešlo o phishing). Ve většině případů se přitom strany nějakým způsobem dohodnou, případně výrobce ustoupí ze svého požadavku, zvláště pokud uzná, že by v dané situaci neměl dobrou důkazní pozici.

Někdy nicméně softwarový výrobce začne uplatňovat i právo na audit (kontrolu) všech zařízení firmy. Licenční či všeobecné obchodní podmínky softwarových firem toto právo ve většině případů skutečně obsahují. Otázkou ovšem je, zda při instalaci nelegálního softwaru byly takové licenční podmínky vůbec uzavřeny. Logicky nikoliv, neboť základním předmětem licenční smlouvy je právě udělení oprávnění (licence) poskytovatelem nabyvateli. S požadavkem na audit se proto většinou lze v praxi setkat např. u subjektů, které sice zakoupily legální licenci, ale použily ji na více počítačů, než jim podmínky povolovaly, nebo které

zapomněly původní software s propadlou licencí odinstalovat.

V horším případě mohou být jak společnost (neboť i právnické osoby jsou podle českých právních předpisů trestně odpovědné), tak i jednotlivci vyšetřováni policií a souzeni v trestněprávním řízení pro porušení autorského práva. Podle § 270 trestního zákoníku (zákon č. 40/2009 Sb.) platí, že uvedený trestný čin spáchá ten, kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu.

Pokud by vznikla škoda velkého rozsahu (dosahující nejméně deseti milionů korun), hrozí trest odnětí svobody až na osm let. Nutno říci, že ke spáchání tohoto trestného činu je zapotřebí úmyslu. Pokud by došlo k porušení autorského práva z nedbalosti, bylo by možné potrestat viníka pouze za spáchání přestupku. V praxi jsou přitom zpravidla ukládány podmíněné tresty odnětí svobody, příp. další tresty jako zákaz činnosti, zabavení a propadnutí počítačové techniky.

Asi neprozradím nic nového, když uvedu, že prevence těchto komplikovaných situací v podobě efektivního software asset managementu je pro firmy zcela zásadní. Může jít například o:

- přijetí interní dokumentace (např. směrnice), která zakazuje instalaci jakéhokoli softwaru bez souhlasu zaměstnavatele,
- pravidelná školení (nejen při nábory zaměstnanců),
- zavedení technických a organizačních opatření v souvislosti se zabráněním instalace softwaru bez souhlasu administrátora a pravidelné kontroly,
- zavedení pouze kontrolované firemní výpočetní techniky (zákaz BYOD) či
- prověření distributora (prodejce) licence, potažmo legality licencí před zakoupením.

Sečteno a podtrženo: vždy platí zlaté heslo „důvěřuj, ale prověřuj“. Bez kontrolních mechanismů a pravidelných softwarových auditů firmy riskují. Pokud však zavedou dostatečná opatření, mají i dobrou šanci vyvinut se z případné žaloby za porušení autorského práva zaměstnancem. ■

Autorka je advokátka, Röd & Partner, advokáti

Pokud by vznikla škoda velkého rozsahu (dosahující nejméně deseti milionů korun), hrozí trest odnětí svobody až na osm let.