



Zabezpečení cloudu pro zdravotnické služby

Zdroj: <https://ec.europa.eu/digital-single-market/en/news/study-cloud-security-healthcare-services>

Zdravotnický sektor prochází procesem digitalizace a neustále přijímá nové technologie k dosažení provozní dokonalosti. Integrace nových technologií do již tak složité IT infrastruktury otevírá nové výzvy, týkající se ochrany údajů a kybernetické bezpečnosti. Probíhající pandemie COVID-19 byla dalším katalyzátorem kybernetických útoků na zdravotní péči. Typickými příklady jsou phishingové útoky. Tato pandemie současně zdůrazňuje potřebu služeb vzdálené zdravotní péče, protože systém byl v některých zemích ohromen a fyzická přítomnost byla rizikem pro šíření pandemie. V této souvislosti cloudová řešení poskytla pružnost a rychlý přístup k zavádění nových služeb, včetně „virtuálního“ zdraví a telemedicíny.

Tato studie si klade za cíl poskytnout cloudové bezpečnostní postupy pro zdravotnický sektor a identifikovat jeho bezpečnostní aspekty, včetně příslušných aspektů ochrany údajů, které je třeba zohlednit při nákupu cloudových služeb pro zdravotnický průmysl. Sada obecných postupů si klade za cíl pomoci IT profesionálům v kontextu zabezpečení zdravotní péče vytvořit a udržovat cloudové zabezpečení při výběru a nasazení vhodných technických a organizačních opatření.

Identifikace příslušných hrozeb a rizik pro cloudové služby ve zdravotnickém průmyslu a požadavky na bezpečnost a ochranu údajů jsou rovněž zahrnuty v rozsahu této zprávy. Mezi další cíle patří prezentace informativních a praktických případů použití a jejich analýza relevantních hrozeb a opatření cloudové bezpečnosti. Celkovým závěrem odvozeným ze studie je integrace cloudu ve zdravotnictví. Některé zdravotnické organizace však váhají s přijetím cloudových služeb, protože jsou zpochybňovány hustým a složitým právním základem a novými technologiemi. Někdy dochází ke ztrátě správy dat a zpracování osobních údajů v cloudu. Některé zdravotnické organizace používají **PaaS** (úplné prostředí pro vývoj a nasazení v cloudu, které poskytuje prostředky umožňující dodat cokoli od jednoduchých cloudových aplikací po propracované podnikové aplikace s podporou cloudu) pro propojení zdravotnických prostředků s webovou aplikací pro vzdálené monitorování pacientů nebo **SaaS** (model nasazení softwaru, kdy dochází k hostování aplikace provozovatelem služby) pro dokumentaci a plánování konzultací mezi lékařem a pacientem. Studie je strukturována kolem tří případů použití, které jsou nejvýznamnější při používání cloudu nebo k budoucímu používání, zejména elektronického zdravotního záznamu, vzdálené péče a lékařských zařízení.

Zpráva agentury ENISA vychází z toho, jak Evropská komise letos postupuje vpřed s iniciativou [European Health Data Space](#) na podporu bezpečné výměny údajů o pacientech a přístupu k údajům o zdraví.

Pandemie COVID-19 podtrhla zvýšenou potřebu efektivních a bezpečných digitálních zdravotnických služeb. Cloudová řešení umožňují flexibilní a rychlé nasazení elektronického ukládání dat a elektronických komunikací, jako je telemedicina. Složitost právních systémů

a nových technologií i obavy o bezpečnost citlivých údajů o pacientech však zpomalily odvětví zdravotnictví při přijímání cloudových služeb.

[Zpráva](#) řeší tyto problémy tím, že poskytuje bezpečnostní pokyny pro tři hlavní oblasti, v nichž jsou cloud služby používané v oblasti zdravotnictví, a to na:

- **Electronic Health Record (EHR)**, tj. Systémy zaměřené na sběr, ukládání, správu a přenos zdravotních údajů, jako jsou informace o pacientech a výsledky lékařských vyšetření;
- **Vzdálená péče**, tj. Podmnožina telemedicíny podporující vzdálené konzultace pacienta a lékaře;
- **Medical Devices**, tj. Cloudové služby podporující provoz zdravotnických zařízení, jako je zpřístupňování údajů o zdravotnických zařízeních různým zúčastněným stranám nebo pro monitorování zařízení.

U každého z těchto případů použití zpráva zdůrazňuje hlavní faktory, které je třeba vzít v úvahu, když zdravotnické organizace provádějí příslušné hodnocení rizik, například pokud jde o riziko pro citlivé údaje o pacientech nebo dostupnost lékařské služby. Tyto pokyny jsou však pouze prvním krokem, aby se poskytovatelé zdravotní péče mohli bezpečně přizpůsobit cloudu. Je zapotřebí větší podpora, například zavedené průmyslové standardy v oblasti cloudového zabezpečení, konkrétní pokyny od vnitrostátních orgánů a orgánů EU a další pokyny orgánů pro ochranu údajů týkající se přenosu údajů o zdravotní péči do cloudu.

Zpráva rovněž navrhuje soubor bezpečnostních opatření, která mají zdravotnické organizace implementovat při plánování svého přechodu na cloudové služby, jako je vytváření procesů pro správu incidentů, definování požadavků na šifrování dat a zajištění přenositelnosti a interoperability dat. Opatření jsou navržena s ohledem na [návrh kandidátského systému certifikace kybernetické bezpečnosti EU v cloudových službách \(EUCS\)](#), aby byla zajištěna kompatibilita a mapování požadavků. Návrh systému agentury je součástí rámce certifikace kybernetické bezpečnosti zaměřeného na posílení důvěry v produkty, služby a procesy ICT v celé Evropě. Návrh režimu je otevřen pro veřejné konzultace do 7. února 2021.