21. 8. 2014

ID: 95126

Jsou data v advokátních kancelářích opravdu v bezpečí?

Komerční sdělení

Právníci i advokáti jsou si sice vědomi toho, že data klientů jsou důvěrná, nicméně už si nemusí uvědomovat, jak snadné je se dnes k těmto datům dostat. Nejspíš komunikujete s klienty pomocí e mailů a data máte uložena na svém počítači, případně na serverech v kanceláři. Ale je to bezpečné? Při zapojení cloudu se rizika výrazně snižují.

Obliba cloudu dnes roste, jak dokazuje i jeho obliba mezi tzv. virtual lawyers. Je to dáno především možností okamžitého přístupu k datům, faktorem nižších nákladů na informační technologie a pro advokátní kanceláře tak důležitou vysokou úrovní bezpečnosti dat. V zásadě můžeme aspekty bezpečnosti dat uvnitř cloudu rozdělit na tři části. Fyzickou, on line a právní.

Fyzická bezpečnost

Z hlediska fyzického zabezpečení se jedná o vytvoření takového prostředí, ve kterém budou uloženy servery se zákaznickými daty. Toto je velmi důležitá část celé bezpečnosti, protože poskytovatel musí nejenom zajistit dostatečně velké množství úložného prostoru, ale zároveň musí dbát na to, aby se k němu nedostal nikdo nepovolaný. Za tímto účelem tak vznikají celá datová centra, pečlivě střežená personálem i nejmodernější technikou, a to mnohdy až na armádní úrovni zabezpečení.

„Snad na všech obchodních schůzkách se nás právníci ptají, jak je to s bezpečností jejich dat v aplikaci SingleCase," říká Pavel Krkoška ze společnosti SingleCase, která poskytuje software pro správu spisu. „Z hlediska fyzického zabezpečení jejich dat jim vysvětlujeme, že datová centra společnosti Amazon, na kterých budou jejich data uložena, jsou chráněna fyzickými zabezpečovacími mechanismy včetně vojenského perimetru, kam je povolen vstup pouze osobám s příslušnou úrovní oprávnění."

Online bezpečnost

Cílem **online bezpečnosti** je zajistit, aby nikdo nepovolaný virtuálně nepronikl elektronickou cestou dovnitř serverů a nemanipuloval se zákaznickými daty. Poskytovatelé cloudu k tomu využívají celou řadu nástrojů, od řízení práv v aplikaci, přes šifrování dat, až po zapojení hardwarových firewallů (což jsou specifická zařízení, která analyzují provoz na síti a zajišťují její ochranu). Někteří poskytovatelé používají pokročilé nástroje v kombinaci s penetračními testy na úrovni bankovního zabezpečení, což ve výsledku zaručuje prakticky neprolomitelnou ochranu dat zákazníka.

Právní bezpečnost

Právní aspekty cloudové bezpečnosti jsou celkově složitější. Jelikož se jedná o poměrně novou technologii, zákony týkající se bezpečnosti jsou vytvářeny za běhu. Jak uvádí ve své studii organizace BSA (Business Software Alliance): *„Země po celém světě zlepšují právní prostředí pro cloud computing, avšak děje se to nevyrovnaným tempem*."

Nicméně po rozsudku Městského soudu v Praze ve věci uprchlého podnikatele Františka Savova se situace cloudu a právní bezpečnosti u nás trochu zkomplikovala. V rozsudku soud argumentuje, že cloud není místem výkonu advokacie, a tedy nepožívá zvláštní ochrany. S tím však nesouhlasí řada právníků. Oproti české judikatuře, ve které pojem cloud v podstatě není zachycen, je evropská judikatura již mnohem dále. Evropská komise (EK) na podporu cloudu dokonce sestavila skupinu odborníků, která má za úkol vypracovat bezpečné a spravedlivé podmínky smluv o poskytování služeb cloud computingu. Jejím smyslem je vyjasnění podmínek používání cloud computingu tak, aby byly odstraněny obavy z jeho používání z důvodu nejasnosti smluv o poskytování služeb. Jde o další krok EK na cestě k podpoře širokého využívání potenciálu cloud computingu a Česká republika se tomuto trendu bude muset brzy přizpůsobit.

Data v kanceláři vs. cloud – 2 mýty o bezpečnosti dat v kancelářích

V předchozím textu popisujeme vysokou úroveň zabezpečení cloudových služeb. A jak je na tom ve srovnání bezpečnost dat v běžné právní kanceláři? Zaměřili jsme se na dva nejčastější mýty s ní spojené.

Mýtus č. 1: K datům posílaným e-mailem se nikdo nepovolaný nedostane

Citlivá data opravdu není vhodné zasílat pomocí obyčejných e-mailů.

- 1) E-mail se posílá v 99 % případů v prostém textu (nezašifrovaný), tedy se dá po cestě mezi odesílatelem a příjemcem přečíst nebo dokonce změnit.
- 2) I dnes je velice snadné poslat e-mail jménem někoho jiného, zvládne to každý schopnější „ajťák“.

Pokud nechcete, aby vaše citlivá data procházela kontrolou, popř. byla dokonce zneužita, mějte je uložena v bezpečném úložišti a pouze na ně v interní komunikaci odkazujte. Můžete také využít některé z na trhu dostupných řešení pro šifrování e-mailové komunikace.

Mýtus č. 2: Data jsou v mé kanceláři zaručeně v bezpečí

Z hlediska bezpečnosti je na tom cloud mnohem lépe i v porovnání s ukládáním dat na vlastních serverech ve firmě. Jenom si představte situaci, kdy se někdo rozhodne, že vám nějaká data odcizí. I kdybyste měli neprůstřelnou ochranu v podobě špičkových firewallů a šifrovaných přenosů dat, pořád jsou tu ještě vaše servery. A pokud jste menší firma, pravděpodobně máte servery uloženy někde ve svých kancelářích, často přímo pod vaším stolem. Případy, kdy se někdo vloupal do kanceláře a servery, nebo jen pouhý disk, jednoduše odnesl, jsou realitou. Pokud nejsou disky stále zašifrované, pak nepotřebuje žádné speciální vybavení, aby se jednoduše zmocnil vašich dat. A to se bavíme o krajní variantě fyzického zcizení. Mnohá firemní řešení on-line bezpečnosti jsou totiž pro zkušenější hackery jen otázkou času.

Pokud budete mít svá data uložena na cloudu, velká část těchto starostí vám odpadne. **Poskytovatelé cloudových služeb dnes rizika aktivně hlídají a svou bezpečnost neustále testují.** Důvod je prostý - bezpečnost dat jejich zákazníků je pro ně na prvním místě, pokud by totiž došlo k jejímu narušení, pak by to pro ně znamenalo konec byznysu.

To je i případ serverů, které jsou využívány pro SingleCase. Zákaznická data jsou uložena v datových centrech společnosti Amazon, která využívá nejmodernější bezpečnostní technologie. Díky tomu jsou klientská data v bezpečí – a to jak z hlediska případných on-line útoků, tak i fyzických pokusů o krádež. Máte-li však opravdu spolehlivé IT oddělení a zajištěnou interní bezpečnost, pak není problém, aby byla data ze SingleCase ukládána přímo u vás. S jejich migrací vám rádi pomůžeme!

Další články:

- LEAGLE.ONE: Triangle Family Office #12: Skrytá slabina úspěchu: zakladatelský paradox v řízení bohatství
- Prémiový rezidenční komplex Bakers Court přináší na realitní trh komfortní bydlení s 5* službami
- ESG Simple jako praktická opora pro ESG reporting malých a středních podniků
- Partner BBH Tomáš Sedláček obdržel prestižní ocenění „Lawyer of the Year“ na IFLR Europe Awards 2026 v Londýně
- LEAGLE.ONE: Kdo pomůže dětem vybrat správnou cestu, když dnešní profese zítra nemusí existovat?
- Jindřich Fuka novým advokátem Aegis Law
- LEAGLE.ONE: Advokacie po nástupu AI: Kdo se přizpůsobí, získá náskok. Kdo ne, může zůstat pozadu
- Digitální důkazy z webu v soudním řízení: jak doložit, co bylo online zveřejněno?
- Český Deloitte Legal posiluje: Jiřina Procházková jmenována CE partnerkou
- V lednu přišel šok. Ze seznamu zmizely tisíce soudních překladatelů
- LEAGLE.ONE: Triangle Family Office #11: Mezigenerační převod majetku: Největší chyba je neudělat nic