31. 5. 2016

ID: 101635

Technologie pro právníky: Nebezpečí ztráty dat 1 - Prevence

eFocus

Každá společnost, bez ohledu na svou činnost, velikost a obrat, spravuje obrovské množství informací, což je aktivum, které má v dnešní době neocenitelnou hodnotu.
Společnosti působící například v sektoru práva a souvisejících oblastech navíc podléhají přísnějším závazkům v oblasti důvěrnosti, profesní mlčenlivosti a ochrany údajů třetích stran, což by mělo vést k zavádění nezbytných opatření k ochraně před ztrátou dat, protože tyto společnosti bývají lákavým cílem pro pachatele počítačové trestné činnosti.

Ještě pořád si myslíte, že naše databáze nejsou tak cenné a že důvěrné informace našich společností nejsou ohroženy?

Možná tak uvažují společnosti, které o ně nikdy nepřišly.

Řeč je o důležitých či dokonce citlivých údajích obsažených v záznamech a dokumentech týkajících se našich klientů v různých právních věcech, ve smlouvách mezi třetími stranami, v důvěrných a často strategických sděleních, dále o chráněných údajích vedených personálním oddělením firmy ohledně bezpečnosti a ochrany zdraví při práci, o údajích od našich dodavatelů, finančních údajích, údajích týkajících se výsledovek, prognóz růstu a obchodních příležitostí, statistických údajích a marketingových plánech atd., jejichž náhlá ztráta má své důsledky.

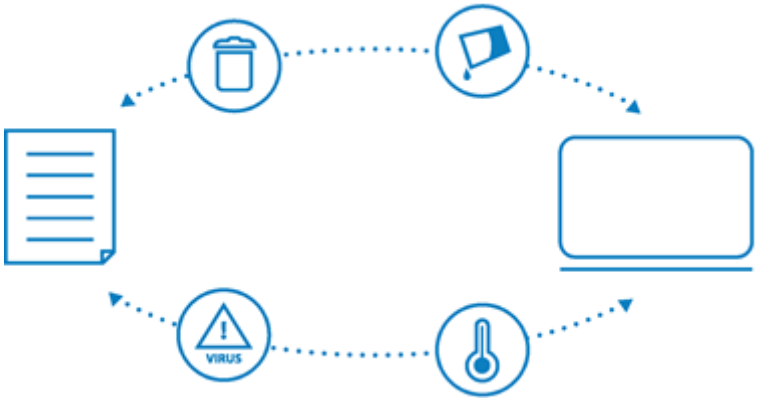
V závislosti na typu ztráty či poškození dat způsobeného společnosti a/nebo třetím stranám, na naší schopnosti zajistit jejich obnovu a na době strávené touto činností mohou **důsledky ztráty informací sahat od úplného ochromení naší běžné činnosti**, a tím ohrožení její kontinuity, což může znamenat jak závažné poškození naší pověsti, tak značné ztráty v případě nároků třetích stran, **po pokuty a sankce uložené kvůli absenci náležité péče o jejich ochranu**.

To, že nešlo o úmyslné zavinění, nijak nezbavuje právní odpovědnosti za ztrátu nebo prozrazení dat třetí strany ani ji nijak nesnižuje.

Prevence znamená snižování rizik a umožňuje nám pracovat s klidnější myslí.

Díky mobilitě a konektivitě pracujeme hned s několika zařízeními. Používání mobilních zařízení nám sice umožňuje přístup k důvěrným údajům našich společností a klientů, umožňuje jej však zároveň i třetím stranám.

Proto se **veškerá preventivní opatření přijatá za účelem minimalizace rizika ztráty dat musí vztahovat na všechna zařízení a počítače společnosti s přístupem k daným údajům**. Všechna bez výjimky.



Jaká opatření je třeba přijmout pro minimalizaci rizika ztráty dat?

1. V intervalech a způsobem stanoveným v plánu zabezpečení informací / na média v něm stanovená **zálohovat soubory, internetové stránky, databáze, data v cloudu a datové** soubory obsažené **na všech zařízeních a počítačích**.

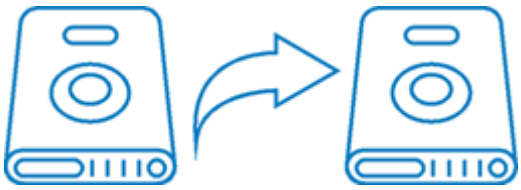
Nainstalovat a aktualizovat **zálohovací software pro servery**.

Nejlepší je, pokud poskytovatel databázového úložiště a/nebo počítačových služeb odpovědný za zajišťování údržby každý den vytvoří jednu nebo více obousměrných kopií v závislosti na objemu dat, která organizace zpracovává, jak je dohodnuto ve smlouvě o poskytování služeb.

Dále je nutno vytvářet zálohy stanovené v bezpečnostním plánu na externí médium/média, přičemž osoba pověřená tímto úkolem by měla v intervalech stanovených pro každý jednotlivý případ odnášet pořízenou kopii/kopie z pracoviště, a tím diverzifikovat rizika a zabezpečovat více kopií nejaktuálnější verze zašifrovaných informací.

Pokud jde o **média**, každá organizace si může v závislosti na objemech ukládaných dat rozhodnout, zda si bude vytvářet vlastní kopie v podobě zkomprimovaného souboru uloženého na USB zařízení, které obvykle není připojeno k žádnému počítači či serveru. Toto řešení má tu nevýhodu, že na to musí někdo pamatovat, je to časově náročné a není možné uložit celý obsah počítače, jako spíše pouze některé soubory a dokumenty, nemluvě o bezpečnostních problémech souvisejících s uchováváním souborů.

Snad nejmoudřejší, co bychom mohli udělat, je ukládat tyto kopie na externí pevné disky s větší kapacitou, které můžeme uchovávat zašifrované a do jisté míry fyzicky zabezpečené.



Nevýhodou zálohování na cloudová úložiště OneDrive, Dropbox nebo iCloud je nízká paměťová kapacita, kterou nám tato úložiště nabízejí, stejně jako nedostatek bezpečnosti těchto cloudů závisející také na tom, jak takovou kopii uložíme (zašifrovanou nebo nezašifrovanou) a jak je nakonfigurováno nastavení soukromí a zabezpečení našeho účtu.

Začínají se objevovat národní cloudové služby, které poukazují na to, že jejich servery se nacházejí ve Španělsku/Evropě, a přijímají vůči organizacím větší odpovědnost za tyto druhy rizik, než je odpovědnost spojená s běžnými nástroji, které nám někteří z větších operátorů nabízejí standardně, zdarma a snadno.

2. Před aktualizací softwaru se doporučuje vytvořit kompletní zálohu a otestovat ji, abychom se ubezpečili, že v případě poruchy budeme schopni dané informace obnovit. To se týká také aktualizací internetových stránek.

3. Nejčastějšími problémy spojenými s hardwarem, při kterých dochází ke ztrátě informací, jsou výpadky napájení. Dobrým preventivním opatřením proti vzniku takových problémů je **používání záložních zdrojů energie na serverech**.

4. Ochrana a zašifrování počítačů a mobilních zařízení pomocí šifrovacího softwaru představuje další způsob omezení přístupu, který by bylo nutno překonat ještě předtím, než zapneme počítač a pomocí hesla vstoupíme do systému.

5. Ochrana a zašifrování důležitých a důvěrných souborů pomocí hesel, zejména pokud tyto soubory obsahují data, při jejichž zpracování jsme vázáni zvláštní povinností ochrany podle zákona o ochraně osobních údajů (LOPD). Kromě toho musíme v takovém případě znát heslo pro přístup k těmto dokumentům, jejich ukládání na USB zařízení a zasílání e-mailem, což zesiluje ochranu informací před přístupem ze strany neoprávněných osob nebo pracovníků firmy zaměstnaných pouze na přechodnou dobu.

Pokud v některých částech roku najímáme brigádníky, má tento druh šifrování dokumentů velký význam. Tito zaměstnanci by měli dostat dočasné
heslo, které jim umožní přístup k souborům a jehož platnost vyprší ukončením pracovního poměru v naší firmě. Tento druh šifrování umožňuje, máme-li zájem, sledovat přístupy k dokumentu z různých terminálů, což představuje další kontrolní mechanismus.

Tento drobný detail, který může být tak jednoduchý jako zadání hesla do možností uložení, není jen bezpečnostním opatřením, ale také opatřením, které posiluje dobrou pověst naší firmy. Pokud klientovi zavoláte, abyste mu sdělili heslo pro přístup ke smlouvě, vzbudíte v něm velkou důvěru, protože klient vidí, že se jeho právník opravdu snaží chránit jeho informace a poskytuje mu osobnější servis.

6. Operační systémy, aplikace, antivirové programy a firewally mějte na všech zařízeních a počítačích vždy aktualizované. Aktualizace obvykle obsahují tzv. záplaty, které zajišťují ochranu zranitelných míst a chrání před možnými útoky nebo závadami.

7. Instalujte a **pravidelně aktualizujte program na obnovu dat**. Nejspolehlivějším preventivním opatřením je předplatit si služby obnovy u poskytovatele databázového úložiště a/nebo služeb počítačové údržby, který disponuje znalostmi a nástroji obnovy využívajícími celou řadu metod, což zajistí lepší obnovu dat, než o jakou bychom se my sami snažili metodou pokus-omyl.

8. Nepřetěžujte pevný disk počítačů a serverů. Využití služeb datového úložiště v cloudu je v současnosti jedním z nejčastějších doporučení. Musíme však pamatovat na bezpečnostní opatření při zálohování do cloudu, právní požadavky, které se na nás vztahují, a skutečnost, že svěřujeme tato data do úschovy externímu poskytovateli, se kterým uzavřeme smlouvu stanovující přesný rozsah jeho případných odpovědností.

Naší odpovědností je také konfigurace účtu uživatele služeb úložiště v cloudu. Ověřením zabezpečení a soukromí účtu a jeho konfigurací v rámci maximálních parametrů, stejně jako ukládáním zašifrovaných souborů, si můžeme v této oblasti ušetřit mnoho problémů.

9. Mažte nepoužívané soubory a aplikace.

10. Na pracovišti s počítači udržujte **vhodné podmínky prostředí** odpovídající pokynům výrobce/dodavatele provádějícího instalaci (stabilní teplota, vlhkost a čistota).

11. Servery a paměťové jednotky by měly být **fyzicky zabezpečeny** proti přístupu ze strany neoprávněných osob. Nejčastější metodou ochrany bývá to, co známe pod označením „lednička s klíči“.

12. Počítače, zařízení a paměťové jednotky by měly být na konci předpokládané **životnosti** nahrazeny novými, protože jejich delší používání by mohlo vést k paměťovým nepřesnostem, a tím i ke ztrátě dat.

13. Podporujte interní kulturu odpovědnosti za bezpečnost informací s trendem minimalizace rizik úniku dat:

- a. Poznamenejte si čísla IMEI mobilních zařízení pro účely zablokování a nahlášení v případě ztráty, loupeže nebo krádeže.
- b. Pravidelně měňte PIN mobilních zařízení; aktivujte kódový zámek, pokud nebudete zařízení po krátkou dobu používat.
- c. Měňte heslo routeru a, je-li to možné, dbejte na to, aby neobsahovalo Vaše jméno nebo firemní prvky, které by umožnily snadno zjistit přístup k Vaší WiFi.
- d. Chraňte přístup k počítačům a zařízením, stejně jako ke všem účtům v aplikacích, silnými a různými hesly a relativně často je měňte.
- e. Aplikace stahujte pouze z oficiálních internetových stránek a věnujte velkou pozornost autorizacím a souhlasům, které staženým aplikacím udělujete, co se týče přístupu k datům uloženým na Vašich zařízeních a případného zpracování Vašich dat, ke kterému dáváte souhlas.
- f. Varujte před rizikem používání firemních souborů a dat ve veřejných a otevřených sítích WiFi, protože v případě, že spojení není zašifrované, se vystavujete vážnému riziku, že se stanete obětí krádeže hesla nebo dat.
- g. Poskytujte aktuální informace o nejčastějších počítačových útocích nebo virech a zajistěte, aby všichni členové týmu věděli, že nesmějí otevírat odkazy uvedené v SMS nebo e-mailech

zaslaných z neznámých účtů, a nenechali se zlákat nabídkami a slevami z cen produktů, které nebyly pořízeny od subjektů, kterým jsme nedali souhlas k zasílání komerčních informací (spam).

- h. Nikomu neposílejte automatické zprávy s oznámením, že během dovolené budete mimo kancelář, a nedávejte na sociální sítě fotografie z dovolené.
- i. Šiřte informace ohledně nevhodnosti používání USB flash disků a podobných zařízení neseriózních nebo neznámých třetích stran. Přístup malware do Vašeho počítače prostřednictvím USB flash disků, včetně tzv. keyloggerů, je jedním z nejčastějších rizik spojených s USB flash disky, protože tato zařízení mohou snadno detekovat hesla používaná pro přístup k důvěrným informacím, aniž bychom si toho vůbec všimli. Nejlepší je udržovat USB flash disky mimo dosah, pokud to fyzické uspořádání našeho pracoviště umožňuje.

Existuje vážné riziko, že se staneme oběťmi krádeže hesla nebo dat!

Jaká jsou opatření, naplní-li se nejhorší scénář a dojde ke ztrátě dat?
Dočtete se v dalším díle Technologie pro právníky.

Wolters Kluwer ČR, a. s.
www.kleos.cz

Další články:

- Recenze publikace: Chalupa, R. Zákon směnečný a šekový – komentář směnečné části. Zákon o mezinárodním právu soukromém – komentář směnečné části. Praha: Leges, 2021, 646 s.
- Recenzia
- Budoucnost je v technologiích i udržitelnosti
- Anotační recenze: Vyvlastnění a vyvlastňovací řízení
- Věznice jsou přeplněné a věznění příliš drahé. Knihou Tresty budoucnosti chce INFO.CZ otevřít diskuzi o změnách
- Recenze na knihu: Zdeňková, V., Seidlová, M., Čornejová, H.,Peterová H.: Jak správně vytvářet a využívat FKSP: Jak postupovat při poskytování příspěvku na stravování.
- Recenze na knihu: Zuzana Strnadová: Co by měl vědět příjemce dotace. 1.vyd. Praha: GRADA

Publishing, a.s., 2019, ISBN: 978-80-247-3076-9

- Ondřej Chmela: Zrušení poplatku za podnět k ÚOHS lze považovat za správné
- Anotační recenze: Koudelka, Z., Průcha, P., Zwyrtek Hamplová, J.: Zákon o obcích (obecní zřízení) – Komentář. Praha: Leges, 2019, 480s
- Pražské finále osmého ročníku konferencí Soukromé právo
- Recenze: Jakub Tomšej a kolektiv – Zaměstnávání cizinců v České republice