Ukládáte data? A víte vlastně kam? – 2. část

O jakých datech je v tomto textu řeč?

Zjednodušeně řečeno, jde o všechna ta písmena a číslice, která ve vašich organizacích někdo naťuká do počítačů. Samozřejmě, k písmenům a číslicím přidejme fotografie a další obrázky, zvukové nahrávky, videa a vůbec všechno, co tvoříte. To všechno jsou data, která vaše organizace vytvořila, vlastní je a zodpovídá za ně.

Dnes to bude o tom, jak si pohlídat data na lokálních a přenosných discích

Nad pojmem „disk" asi v tomto okamžiku ajťáci zaujatě zvedají obočí, protože je nepřesný. Věřím ale, že pro naše potřeby bude dostatečný. Pojďme si tedy potřebné pojmy vymezit.

- Slovo „lokální" tedy znamená, že data jsou uložena uvnitř vašeho počítače a čekají na to, až je budeme potřebovat.
- Případně může jít o data sdílená, která ukládáme na sdílené disky, které tvoří součást vnitřní počítačové sítě organizace. Takto s nimi může pracovat více zaměstnanců podle předem dohodnutých pravidel.
- Slovem „disk" pak můžeme označit úplně libovolnou „věc" na kterou se ukládají informace, ať už leží v počítači nebo jinde v síti.
- Za slovem „přenosný" si pak představme cokoliv, na co ukládáme informace a můžeme to mechanicky přemísťovat. Máte třeba na klíčích flashdisk? Nebo paměťovou kartu ve fotoaparátu? Tak to jsou ony.

V úvodu jen pro pořádek připomenu, že je nejen dobré, ale i nezbytné, abychom měli oddělený svůj pracovní a soukromý život. Nejde jen o to, abychom dokázali fyzicky odcházet z práce a odpočívat, ale také o to, abychom oddělovali svá data.

Jednoduše řečeno – určitě vám nemohu doporučit, abyste si uložili soukromé fotky, naskenovanou sbírku romantických básní z dob svých sladkých sedmnácti nebo třeba rodinné účetnictví na svůj pracovní počítač. A naopak vám rozhodně, ale ROZHODNĚ, nedoporučuji ukládat si „něco z práce" na soukromý počítač. Zvláště pak, pokud to „něco" obsahuje osobní údaje a citlivá data. Tedy pokud jste v časové tísni a vzali jste si domů třeba soubor s docházkou zaměstnanců, abyste mohli připravit podklady pro mzdy, určitě si najděte pro takovou práci jiné řešení (i v tomto okénku se určitě nějaké návrhy objeví), než je uložení souboru na domácí počítač. Dovedete si představit, že ke stejnému počítači sedne jiný člen vaší rodiny a nedopatřením soubor někam odešle nebo ho neobratně zveřejní. Věřte mi, tohle nechcete zažít.

Veškerou techniku, která obsahuje důležitá data, důsledně chraňte bezpečnými hesly, zamykejte počítač kdykoliv od něj vstáváte. Soubory s citlivými údaji přenášejte zašifrované nebo si je alespoň zajistěte heslem. Doporučuji nenosit „flešky" po kapsách, neválet je po stolech. Svět je plný neveselých historek, v nichž se na půjčených discích ocitly v nepovolaných rukou konkurentů velmi důvěrné firemní informace, Podobně, jako si dáváte pozor na své soukromé věci, opatrujte i data.

Zpátky do práce – ještě ke sdíleným diskům

Sdílené disky mohou být dobrý sluha, ale taky špatný pán. Pokud je v organizaci máte, mohou být užitečné. S daty na nich uloženými mohou pracovat malé i větší skupiny zaměstnanců. Můžete tak mít na jednom místě dokumenty, které používá váš ekonomický úsek, jinde mohou s elektronickou knihovničkou plnou inspirativních příkladů pracovat aktivizační pracovnice, další prostor může být vyhrazen třeba pro

management, řízení kvality, nebo pro zavádění biografického přístupu do individuální práce s klientem. Že to znáte a občas se v duchu ptáte, jestli to čirou náhodou nemá nějaký háček? Hned celá skupinka háčků by se dala najít.

- Nejdůležitější je myslet na to, aby měli zaměstnanci přístup právě a jenom ke svým dokumentům. Nemělo by se stát, že sociální pracovnice s úžasem zabloudí do dat čerpání rozpočtu organizace.
- Pokud používáte sdílené disky, je potřeba mít k nim dohodnutá a sepsaná pravidla pro přidělování přístupů. Často se označují výrazem politiky přístupů.
- Nezapomeňte ani na to, že takové disky musí určitě mít někde své zálohy, abyste o data nepřišli. Určitě je rád a dobře zajistí IT odborník. Pokud se ovšem dozví, že takovou věc řešit má.
- S disky musí být možné dobře pracovat. Pokud někteří zaměstnanci pracují na více počítačích, měli vy být schopni přihlásit se z každého z nich. Pracuje někdo mimo vnitřní síť organizace, třeba z domu? Pak potřebuje mít možnost otevřít si bezpečnou cestu. Samozřejmě, že taková existuje, bývá označována jako „VPN“. Mimochodem, právě takovéto připojení je jednou z možností, jak se dostat k pracovním datům a současně si je „netahat“ na soukromý počítač. Jak je možné si takovou „vé-pé-enku“ představit? Pokud si můžeme vnitřní síť představit jako opevněnou tvrz (řekněme, že to tak opravdu je), pak VPN je soubor opatření, k nimž patří klíč, kterým si může otevřít dvířka jeden konkrétní uživatel. Po odemčení se vytvoří bezpečný „tunel“, kterým se data přesouvají v zašifrované podobě. Pro případné lupiče a piráty, kteří se snaží do „tvrze“ proniknout z internetu, je takový kanál obtížně napadnutelný. Jakmile se od VPN počítač odpojí, pomyslná dvířka se zamknou a kanál uzavře. Opevnění se zase stane neproniknutelným. (Pokud někdo v minulosti používal připojení prostřednictvím vzdálené plochy, věřte, že to znamenalo, že jste do organizace procházeli doširoka otevřeným oknem a vesele trousili informace divokým internetem.)

Možná je čas, abychom si položili pár otázek. Víte vlastně, jakým způsobem se k datům a systémům svého zaměstnavatele připojujete vy? Kde máte uloženy informace? Kolik vlastníte flashek, co je na nich a kde vlastně jsou? A máte v organizaci sepsaná pravidla pro práci na sdílených discích?

Máte přehled o tom, která vaše data zamířila mimo organizaci a jsou uložena někde v cloudu? Tak o tom zase příště.