

Ve jménu bezpečnosti aneb Jak končí dobré myšlenky

Konečně přichází dlouho očekávaný okamžik. Nový zaměstnanec velké korporace si láskyplně vybalí zbrusu nový notebook posledního typu. S uspokojením si povšimne, že aktivní displej je ještě větší než displej jeho předchozího počítače. Také procesor je silnější a grafická karta s hardwarovým akcelerátorem jako by ani nebyla určena k psaní textů a tabulek...

Vše spíše vyzývá k přehrávání DVD a provozování multimediálních aplikací. Spolu s notebookem přicházejí i standardní firemní aplikace: MS Office, Outlook, Internet Explorer. Zaměstnanec nakonec dostane přidělen i svůj uživatelský účet, který pro jistotu nemá administrátorské oprávnění. Prý z důvodu bezpečnosti.

První problém - administrace

Problémy na sebe nenechají dlouho čekat. Nelogicky nastavený režim napájení přinutí počítač hibernovat až ve chvíli, kdy už na to nemá energii - disková operace pak skončí tvrdým vypnutím vždy právě v polovině zápisu. Skoro je nám našeho nového notebooku líto. Otevřeme si kontrolní panel, a ejhle - jako "neadministrátor" nemáme na provedení jakékoliv změny nárok. Řešení se naštěstí nabízí: oficiální cesta přes firemní IT helpdesk. Zavoláme milé operátorce, prohodíme pár zdvořilostních frází, pak jí sdělíme své osobní číslo a nakonec i svůj problém. Ona si nás zapíše, přidělí našemu požadavku číslo a vyzve nás, abychom vyčkali příchodu technika. Celá operace netrvala déle než deset minut, a to jsme operátorce stačili i vysvětlit, co je to ten kontrolní panel a co znamená hibernace. Konečně, byla to opravdu milá holka.

Už následujícího dne nám volá technik. Díváme se oba do kalendáře, kdy by to šlo, a vidíme, že už za dva dny by se mohla schůzka podařit. Technik v dohodnutou dobu přijde, přihlásí se k našemu počítači jako administrátor, dvakrát ťukne myší a nastavení změní. Operace je vnitřně vyúčtována a firma si z jedné části do druhé zaplatí několik set korun.

Nějaký čas je opět klid. V pátek odpoledne však zpozorujeme, že se nám najednou nějak viditelně zpomalil počítač. Jako na potvoru se to stane zrovna při obchodním jednání, v době, kdy nejsme připojeni k elektrické síti. Nevěříme svým očím: disk běží naplno, větrák se rozběhl také a představa několika hodin práce na baterie se v mžiku mění na pouhou iluzi.

Příběh ze života

Sám jsem zažil situaci, kdy se jednomu řečníkovi na konferenci během jeho prezentace natolik "zpomalil" počítač, že přestal téměř reagovat. Nakonec onen nešťastník spustil dvakrát po sobě Powerpoint (myslel si, že první ťuknutí myší nebylo dostatečné), a než stačil správně odpovědět na vzniklý "problém sdílení", obě instance programu omylem zase zavřel. Čas jeho přednášky přitom nemilosrdně běžel. Většinu své pozornosti i energie musel přednášející věnovat právě počítači - skoro se zdálo, že neměl čas zabývat se čímkoliv jiným. Začal z toho být nervózní, rozpačitý a prezentaci před mezinárodním fórem nakonec úplně zkazil. Jak by také ne, když mu jeho firemní administrátor nastavil na každý pátek na dvanáctou hodinu kompletní antivirový sken disku. Ten nebožák měl samozřejmě počítač vypnutý a zapnul si jej až těsně před prezentací. Ale právě tím si "naběhl". Program si pěkně počkal na zapnutí počítače a hned vzápětí začal provádět svoji důležitou a neodkladnou práci.

Uživatelská práva aneb Práva uživatele

Jako "pouhý" uživatel notebooku záhy zjistíme, že antivirový program, který náš administrátor tak moudře nastavil, nesmíme vypnout ani přerušit - jediné, co smíme udělat, je vypnout celý počítač. Mezi námi, k tomu vypnutí při bateriovém provozu stejně brzy dojde... Ale co naděláme, je to tak dobře, neboť je tím chráněna naše bezpečnost.

Nakonec máme vždy právo počítač vypnout. Možná by se nám chtělo nesměle namítnout, že v takovém případě nám budou při prezentaci chybět naše pracně připravené slajdy! Zajímá to ale vůbec někoho?

Přizpůsobme se administrátorovi!

Co se tedy dá dělat, sken disku musí být. Je to nakonec pro naši bezpečnost. Přemýšlíme, jak bychom to mohli vyřešit, a nakonec přijdeme na následující možnost: na páteční odpoledne si přestaneme plánovat schůzky mimo firmu. Pak se nám tento malér už nikdy nestane; v ostatní dny přece můžeme pracovat normálně.

Uspokojeni tímto řešením pracujeme tedy normálně ve firmě dále. Linky nás přivedou na technologické zpravodajství BBC a na něm nás zaujme jedna z audio- či videoreportáží. Zkusíme ji otevřít... a v tu chvíli zjistíme další zajímavou věc: tato reportáž není ve formátu Windows Media, ale ve formátu Real One. "Maličkost," objeví se nám na displeji. "Vteřinku vydržte, odsud si můžete nainstalovat správný přehrávač." My ale po dlouhé vteřince zjistíme, že nainstalovat si nemůžeme vůbec nic. Instalace programů je totiž potenciálně nebezpečná a mohla by do firemní sítě vpustit viry, trojské koně nebo jiné zákeřné druhy kódu. Nevadí přitom, že ty skutečně nebezpečné programy se uživatelů obvykle na nic neptají a pro svůj průnik využijí některou z mnoha bezpečnostních děr systému. Počítač se ale musí chránit kompletně, tedy zřejmě i před běžným používáním. Jistota je jistota. Nakonec - je to přece pro naši bezpečnost. Při instalaci se nám proto objeví sdělení "Nemáte dostatečná práva, obraťte se na administrátora sítě". A voláme opět na helpdesk.

Práce se strachem

Tam už to tentokrát ale tak hladce nejde. Firma totiž tento typ požadavku dosud neřešila a nemá na něj zpracovaný proces. Proces musí být, protože když není proces, musel by někdo rozhodnout na svou odpovědnost - musel by například prohlásit: "Real One Player může být instalován, není v rozporu s bezpečnostní politikou firmy." Jenže jakmile jde o bezpečnostní politiku, jde o práci se strachem. Nemyslíme tím přitom strach řadových uživatelů, ale strach pracovníků IT. Každý ze zaměstnanců IT podpory se bojí udělat jakékoliv rozhodnutí, protože v takovém případě by mohl být vyhozen, a to by v dnešní době útlumu na pracovním trhu nebyla žádná výhra. A IT manažer, který by změnu mohl provést, tomu pro změnu obvykle nerozumí. A protože tomu nerozumí, bojí se rovněž rozhodnout, protože by mohl rozhodnout špatně a mohl by jej vyhodit ten nad ním. Navíc má na rozdíl od pouhého pracovníka IT víc co ztratit, což jeho odvaze také nepřidá.

Microsoftu zmíněná situace samozřejmě nijak nevdává. Asi i z toho důvodu odstranil v osmé verzi svého přehrávače Windows Media Player podporu všech souborů firmy Real. Ale to vědí jen ti uživatelé, kteří čtou počítačové časopisy a weby. V nápovědě pro Windows Media Player slovo Real téměř nenajdeme: pouze v právní noticce se mluví o "skutečné firmě". Stránka s "podrobnostmi" k této "chybě" ovšem pouze mlží a uvádí cosi o kodecích, formátech či špatné verzi přehrávače. Je tam plno různých nesmyslných informací, včetně toho, že bychom se mohli pokusit stáhnout kodek, ale ta informace, že náš soubor nebude principiálně přehrán, ať se budeme třeba stavět na hlavu, tak ta tam prostě není. Jen se, uživateli, ještě chvílku potrap! Můžeme tedy experimentovat, pátrat na internetu po správném kodeku, můžeme se i rozčílit - ale jak by řekl klasik, to je vše, co v tom můžeme dělat. Nic nezměníme na situaci, že audiosoubor ve formátu firmy Real je pro Microsoft - a tedy zřejmě i pro naši firmu - "nebezpečný", zatímco audiosoubor ve formátu firmy Microsoft je v pohodě.

Rozdvojme se!

Co tedy můžeme v takové situaci dělat? BBC potřebujeme sledovat pravidelně, ale do internetové kavárny kvůli tomu chodit nechceme; stejně tak se netoužíme dostat do role rebela a "vůdce vzpour zaměstnanců". Nakonec se ukáže, že jedna cesta k řešení přece jen existuje. Pravda, není systémově nejčistší, zato se ale zdá, že vyřeší většinu našich problémů. Podaří se nám totiž získat administrátorský účet na náš vlastní počítač.

Ach, jaký pokrok! Najednou všechno jde. Můžeme si nainstalovat nejen Real One Player, ale dokonce i "nebezpečnou" lištu Google. A je nám dokonce povoleno nainstalovat si vhodnější driver pro svůj monitor v kanceláři, takže si na něm smíme nastavit i vyšší obnovovací frekvenci! Jak nebezpečné a jak vzrušující!

Naše nadšení však začne brzy vychládat. Zjistíme totiž, že i tato cesta má své stinné stránky. Sice již nemusíme volat kvůli každé maličkosti na ochotné call centrum, povídat si s milým ženským hlasem, zapisovat si číslo našeho požadavku, sledovat, jestli na nás nezapomněli, a organizovat si schůzky s techniky (přijde samozřejmě vždy jiný a vždy mu musíme vysvětlovat vše znovu). Výměnou za to se ale musíme rozdvojit. Najednou jsme totiž dva uživatelé každý "z nás" má svůj vlastní desktop, svůj vlastní seznam naposledy otevřených dokumentů, své vlastní nastavení aplikací. Jeden z nás je administrátor, který může nastavovat počítač a aplikace, nemůže však ke svým souborům na podnikovou síť; ten druhý je běžný, tedy nesvéprávný uživatel, který zase nemůže spustit některé své aplikace. Tato situace začíná zavánět schizofrenií. Co je však ještě horší - situace na našich desktopech začíná až příliš nápadně

připomínat neproduktivní situaci ve firemním oddělení IT, plnou nesmyslných žádostí a úkonů. Musíme se neustále přepínat z jednoho uživatele do druhého - v závislosti na tom, zda potřebujeme pracovat s daty, nebo s aplikacemi -, a když se přepneme, musíme vždy hledat naposledy dokončenou práci na "stole" toho druhého. Ovšem abychom to neměli tak jednoduché, ten druhý stůl vidíme pouze v případě, kdy jsme v roli administrátora. S tím nic neuděláme, protože sami sebe jako uživatele definovaného firmou administrovat nemůžeme, k tomu máme přece helpdesk. Stejně tak nic neuděláme s tím, že máme nyní dva seznamy posledně otevřených dokumentů ve Wordu či v Excelu a samozřejmě dvě různé historie navštívených internetových stránek.

Počítač PC byl původně zamýšlen jako nástroj pro jednoho uživatele - odsud písmeno P, tedy personální, osobní. Ale asi jsem ze staré školy, zjišťuji totiž, že dnes už to zřejmě neplatí. V rámci přibývání nesmyslných funkcí přibyla i tato. Ano, můžeme namítnout, že třeba Unix byl multiuživatelský vždy, od svého zrodu; jenomže nesmíme zapomínat, že Unix byl určen pro úplně jiné počítače. Jeho doménou byly velké sálové stroje, tedy nákladná zařízení, která se sdílela mezi desítkami a stovkami lidí. Tam byla možnost více uživatelských účtů přínosem, funkcí, která měla smysl. Ale pro jaké počítače jsou určeny Windows? Windows jsou určeny pro PC, tedy osobní počítače. Proč si toho - proboha - někdo z jejich tvůrců dosud nevšiml? Jaký smysl zde má správa uživatelských účtů? To si jednou budeme nastavovat "uživatele" i na svém PDA či mobilním telefonu?

Lidé, kteří se za nás baví

Ale i když "jsme" zrovna administrátor, neznamená to, že bychom měli vyhráno a že bychom s naším počítačem mohli pracovat bez omezení. Ťukneme na jeden odkaz - a najednou se nám místo internetové stránky zobrazí hlášení firemního internetového filtru. Nevěřičně čteme: "Tato stránka patří mezi zakázané servery, neboť je zařazena do kategorie ‚Cestování‘. Nemáte tudíž právo ji vidět. Pokud si snad myslíte, že ji nezbytně potřebujete ke své práci, obraťte se prosím na - helpdesk!" Aha, tak pokoj tedy není, pořád máme důvod volat na helpdesk. Je to vlastně stále stejné schéma: IT něco zakáže a pak vyvine nákladný a nepříliš fungující mechanismus, jak tento zákaz řešit.

To ale nevádí. Můžeme totiž konečně mít hřejivý pocit: my vlastně nyní máme svého osobního správce internetového filtru! Ba dokonce celý tým lidí, kteří se touto bohulibou činností zabývají! Jak asi vypadá jejich pracovní den? Ráno kafe a pak celý den prohlížení stránek kategorií Zábava, Erotika, Cestování, Sex a kdovíjakých dalších. My pak můžeme mít o to víc času na vlastní práci. A navíc můžeme být v klidu, že bychom se snad omylem podívali na něco, co bychom neměli vidět! Například na jakýkoliv informační zdroj na webhostingovém serveru, na kterém jsou bohužel shodou okolností i stránky s erotickým obsahem. Moc nás to ale trápit nemusí. Pokud si totiž něco chceme nebo potřebujeme opravdu přečíst, samozřejmě můžeme. Stačí danou stránku vyhledat na Google a podívat se například do jeho cache...

Závěr k zamyšlení

Jak tedy fungují dnešní firemní informační systémy? Špatně. Pod záminkou "bezpečnosti" nesmíme s naším osobním počítačem optimálně nakládat. Pokud to obejdeme, dostaneme se do problému rozdělení uživatelů. Proti trojským koním a úniku dat náš počítač stejně není a ani nikdy nemůže být plně zabezpečen. A pokud se chceme podívat na internet, můžeme mít smůlu, protože někdo mohl zrovna tu naši stránku zablokovat. Obsah jakékoliv stránky přitom vidět stejně můžeme, internet vždy nabízí řadu alternativních cest a kopií. Dokonce i čínští cenzori zjistili, že zablokovat jakoukoliv informaci na internetu prostě nejde.

Chtělo by se říci: Používání počítače je potenciálně "nebezpečné" a mělo by se zakázat! Je totiž stará pravda, že jediný skutečně bezpečný IT systém je systém bez uživatelů. Jakékoliv jiné řešení je nebezpečným kompromisem. Tato možnost je samozřejmě nesmyslná, přesto se však zdá, že právě sem směřuje dosavadní vývoj!

Nabízí se naštěstí ještě jeden přístup. Zamyslet se nad tím, jak zabezpečit systém proti domnělým i skutečným hrozbám a přitom umožnit jeho snadné a efektivní využívání. Konečně právě k tomu byl systém vytvořen a právě proto jsme jej zakoupili.

IT systémy jsou součástí našeho světa. Náš svět není dokonalý ani bezpečný, a přesto v něm musíme žít. Každý den jezdíme automobily či autobusy, které nás nemusí dovézt k cíli - a přesto jimi jezdíme. Každý den riskujeme, že budeme okradeni, pokud vyjdeme z domu - a přesto z něj vycházíme. Každý majitel auta riskuje, že mu bude auto ukradeno, ale žádný řidič se nebrání krádeži svého automobilu tím, že mu odmontuje kola a zazdí jej do garáže. Pak by ho totiž nemusel vůbec kupovat.

Jiří Donát