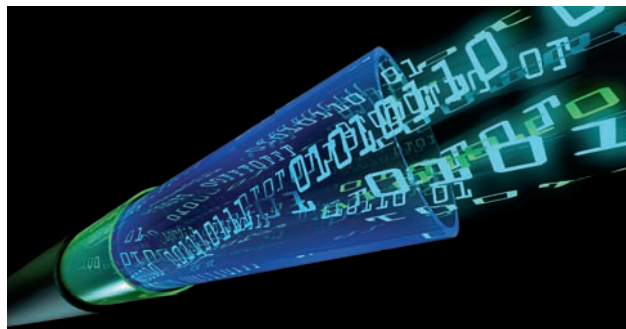


Šifrujte a chraňte podniková data

Celé disky, soubory, sdílená data, e-maily. To dnes není problém zašifrovat, ale důležité je si poradit v situaci, kdy dojde k zapomenutí hesla, ztrátě klíčenky s privátním klíčem, odchodu osoby ze zaměstnání.



Ochrana dat je dnes nedílnou součástí IT a čím dál častěji proniká až ke koncovým uživatelům. Podle zprávy Vontu Risk Assessment celých 43% e-mailových zpráv porušuje bezpečnostní politiku a obsahuje zákaznická data či duševní vlastnictví, data Gartneru pro změnu uvádějí, že 84% nejdražších bezpečnostních incidentů je způsobeno odesláním citlivých dat mimo společnost a 95% rizika způsobují špatně nastavené obchodní procesy a nezpracování uživatelé.

Právě automatické šifrování eliminuje 100% rizika spojeného s porušením bezpečnostní politiky nebo firemních procesů. Z pohledu uživatele se většinou jedná o jednoduchý požadavek typu: „Chci mít zašifrována data a ať se k nim dostanu jen já.“ Tento základní požadavek se však nutně musí dále rozpadnout na celou řadu dalších otázek, jako je „co“, „kdy“, „kde“ nebo také pro „koho“ má být chráněno a „jakým“ způsobem. V podstatě až zodpovězením těchto otázek vzniká základ bezpečnostní politiky, která musí být nutně na začátku jakéhokoliv procesu zavedení a provozu systému ochrany dat. Uvedené šifrování je pak až jednou z celé řady možností způsobu ochrany dat. Pro jednoduchost však nyní zůstaňme jen u šifrování.

Odpovědi hned na první otázku, „co“ chceme chránit, nám většinou vznikají požadavky na ochranu a šifrování textu, souborů, adresářů, disků a komunikace. Zcela záměrně uvádím i komunikace, které nemusí být chráněny jen mezi jednotlivými systémy, a není to tak jen starost ICT oddělení. Všeobecný pohled uživatelů „To mají na starost ti ajťáci“ se tím stává lichý, protože pod ochranou komunikací můžeme rozumět i ochranu před nechtěným přístupem mimo jiné třeba těch zmiňovaných ajťáků. Opět pro zjednodušení příklad elektronické pošty a požadavek „chci šifrovat e-maily“ se musí s ohledem na privátnost

řešit už na straně klienta, a tedy u koncového uživatele. Stejným způsobem se pak musíme dívat i na ICQ nebo obecně instant messaging (IM). Pokud budu pokračovat v uvádění možností, můžeme dále chránit data šifrováním souborů či adresářů nebo také celých disků či textu jako takového.

Dostáváme se k otázce „kdy“. Věřím, že už při výčtu možností co šifrovat vás napadla spousta možností kdy. V této otázce není myšlen přímo nebo jen čas, ale také stav, tj. při vypnutém nebo spuštěném počítači, off-line či připojeném k síti, a to jak LAN, tak i WAN, internet atd.

Hned následně můžeme zahrnout i otázky typu „kde“, částečně související s předchozí otázkou „kdy“, rozšířenou na lokální soubory a adresáře, sdílené složky, disky, USB flashdisky, CD, DVD a celou řadu dalších médií včetně PDA, oblíbených iPhoneů a ostatních mobilních přístrojů. Uf, úplně málo toho není, že? Prakticky se jedná o jakékoliv médium, na které je možné nahrát data, a to nesmíme zapomenout na zálohy a jejich úložiště, která jsou potenciálně nejsnáze napadnutelná.

A na závěr nám chybí zahrnout do skládky pro „koho“ a před „kým“ nebo také „čím“ data šifrovat. Sem zajisté patří jednotliví uživatelé, už uvedení správci systémů a sítí apod. Pod tento bod je ale nutně zahrnout i možné procesy, resp. služby, které mají nebo mohou data využívat, a nejedná se tedy jen o fyzické osoby.

Pokud na všechny uvedené otázky odpovíme, máme před sebou velmi dobrý základ bezpečnostní politiky pro ochranu dat, v našem případě šifrováním. Když navzájem pospojujeme jednotlivé odpovědi, vznikne nám jakási šablona, ze které je třeba vycházet a na ni nalézt vhodné řešení, resp. kombinaci produktů. Nezapomeňme při výběru také na jednoduchou, ideálně