1.7 Bezpečnost datových schránek

1.7.1 Bezpečný přístup k datové schránce

Ke vstupu do datové schránky je nutné přihlašovací jméno a heslo. První poštou doručené heslo si musíte změnit. Nové heslo musí mít nejméně 8 znaků a mělo by obsahovat kombinaci malých a velkých písmen, speciálních znaků (diakritika) a číslic. Přihlašování pod přístupovým jménem a heslem je pouze základní postup. Doporučujeme Vám rozšířit si zabezpečení přístupu prostřednictvím certifikátu zaručujícím bezpečnost používání datové schránky.

1.7.2 Aktualizujte operační systém a bezpečnostní software

Pamatujte, že bezpečný je pouze legální operační systém a bezpečnostní software, který je pravidelně aktualizován. Ideální je forma automatických aktualizací, která nejlépe chrání Váš počítač. Naopak pokud nemáte pravidelně aktualizovaný operační systém a bezpečnostní software, stává se Váš počítač snadným cílem útoku. Zejména Váš internetový prohlížeč, jakožto hlavní brána Vašeho přístupu do datové schránky, nesmí mít žádné tzv. bezpečnostní díry, proto jej udržujte stále aktualizovaný.

1.7.3 K datové schránce přistupujte stejně obezřetně jako k internetovému účtu v bance

Celková bezpečnost datové schránky je dána i Vaším chováním. Rozhodně je namístě při přístupu do datové schránky vypnout všechny tzv. systémy výměny rychlých zpráv, jakými jsou např. programy Skype či ICQ apod., neboť jejich prostřednictvím stahujete obsah i z neprověřených stránek, které mohou Váš počítač poškodit. Při přístupu do datové schránky proto ukončete všechny ostatní aplikace (připojené k internetovým serverům), zavřete internetový prohlížeč, znovu ho otevřete a teprve poté se přihlaste do Vaší datové schránky.

1.7.4 Používejte kvalitní antivirovou ochranu

Pro ochranu před stále novými počítačovými viry je nutné mít legální, kvalitní a pravidelně aktualizovaný antivirový program. Před přístupem do datové schránky zkontrolujte, že máte antivirový software nainstalovaný ve Vašem počítači, že je zapnutý a že obsahuje nejaktuálnější sadu virových definic. Pokud je paměťově rezidentní antivirová ochrana

počítače vypnuta, je okamžitá ochrana nulová. Není-li antivirus aktualizován, stává se Váš počítač snadným terčem virového útoku.

1.7.5 Používejte obousměrný osobní firewall

Firewall je bezpečnostní software, který kontroluje komunikaci Vašeho počítače s ostatními počítači. Některé firewally mohou kontrolovat pouze provoz směrem do Vašeho počítače, jiné kontrolují i provoz, který z Vašeho počítače odchází. Pouze obousměrné firewally ochrání citlivé informace, které prochází přes datové schránky. Při potížích vymažte všechna pravidla a postupným připojováním se k používaným internetovým serverům vytvořte pravidla nová. Kvalitní osobní firewally to umí udělat automaticky, aniž by si vyžadovaly Vaše zadání.

1.7.6 Nepracujte a neprohlížejte internetové stránky pod účtem administrátora

Nikdy nepracujte a nepoužívejte účet administrátora k prohlížení internetových stránek. Při napadení Vašeho počítače by totiž mohlo dojít ke změně jakéhokoliv jeho nastavení a ke kompletnímu převzetí správy systému Vaší datové schránky mnohem snadněji. Účet administrátora by měl sloužit zejména pro správu operačního systému, jako např. pro instalaci nových aplikací apod.

1.7.7 Zálohujte svá důležitá data

Pravidelně zálohujte data uložená ve Vašem počítači. Ztráta osobních dat, včetně dat uložených v systému datových schránek, může být nevratná. Pokud v rámci systému nepoužíváte službu dlouhodobého uchovávání, budou data ve Vaší datové schránce ze zákona smazány po 90 dnech od doručení.

1.7.8 Používejte bezpečné bezdrátové připojení

Bezdrátové sítě se z hlediska bezpečnosti rozdělují na zabezpečené (chráněné hesly, certifikáty nebo klíči) a nezabezpečené (lze se k nim připojit např. v kavárně). Při připojení pomocí nezabezpečené bezdrátové sítě existuje nebezpečí odposlechu komunikace. Z toho důvodu je užitečné změnit konfiguraci takové sítě na zabezpečenou. I když Informační systém datových schránek komunikuje šifrovaně, je v každém případě vhodné přihlašovat se pomocí zabezpečené bezdrátové sítě.

1.7.9 Nedůvěřujte neověřeným zprávám, může se jednat o podvodné zprávy

Informační systém datových schránek komunikuje pouze bezpečným způsobem. Nikdy nepožaduje vložení přihlašovacích, osobních či jiných citlivých údajů do datové schránky odesilatele. Pokud obdržíte datovou zprávu s požadavkem na zadání Vašich osobních dat, jedná se o podvodnou zprávu. Při nastavení notifikace zpráv elektronickou poštou či přes SMS Vám nikdy nebude doručena zpráva obsahující internetový odkaz, tlačítko nebo obrázek, na který lze kliknout. Na takové zprávy v žádném případě nereagujte, informujte o nich prosím pracoviště infolinky a poté je smažte.

1.7.10 Instalujte a užívejte pouze legální software z prověřených zdrojů

Riziko plyne i z instalace neznámých aplikací, jejichž původ nebo skutečné funkce nelze prověřit. Nezáleží na popisu těchto aplikací, ale na ověřitelnosti zdroje a jeho zabezpečení. Existuje totiž řada aplikací, jejichž účelem je implementovat do počítače software, s jehož pomocí mohou být zcizena a následně zneužita Vaše osobní data či Vaše identita v počítači uložená. Základním principem zachování bezpečnosti Vašeho počítače je proto bezvýhradné používání pouze bezpečných a legálních aplikací.