Šifrování

Slovem šifra nebo šifrování označujeme kryptografický algoritmus, který převádí čitelnou zprávu neboli prostý text na její nečitelnou podobu neboli šifrový text.

Ochrana důležitých dat

Šifrování se na počítačích uplatňuje hned několika způsoby. Jedním z nich je například šifrování dat. Data, ať už na pevném disku nebo přenosném médiu, například flash kartě, můžeme šifrovat celou řadou programů. Některé programy, například zdarma dostupný program Truecrypt umožňují dokonce šifrování celého disku, včetně té části, na které je uložen operační systém. Šifrování dat nás chrání především v případě ztráty, či krádeže našeho notebooku, či přenosného média. Mnoho uživatelů dnes na počítačích běžně uchovává citlivé soukromé informace. Také pokud ukládáme v prohlížeči uživatelská jména a hesla k různým službám, musíme počítat s tím, že v případě ztráty či krádeže notebooku, na kterém není zašifrována část disku s operačním systémem, budou naše přihlašovací údaje pravděpodobně kompromitovány.

Vaši poštu nemusí číst každý

Šifrovat však můžeme také e-mailovou komunikaci. I když si zrovna s protějškem nesdělujeme státní tajemství, přesto nemáme zájem o to, aby si naši vzájemnou komunikaci četl někdo další. To bohužel zrovna v případě e-mailové zprávy, která může po Internetu putovat přes různé e-mailové servery, spravované nám zcela neznámými správci, není možné zaručit. Právě proto je vhodné, pokud nám záleží na důvěrnosti zprávy, šifrovat. K tomu můžeme použít například šifrování pomocí PGP klíčů. Nejjednodušším způsobem je pak napsat zprávu například ve wordu, takto získaný soubor následně zašifrovat vhodným programem a zašifrovaný soubor přiložit ke zprávě jako přílohu. Heslo pro dešifrování je pak potřeba druhé straně zaslat jiným způsobem, například prostřednictvím SMS.

Na šifrování jsou také založeny sítě VPN (virtuální privátní sítě), kde jsou šifrovaná data posílána zvláštním kanálem přes veřejný internet. Díky šifrování jsou tato data pro útočníka, který by je někde cestou odchytil, nečitelná. VPN se často používá například pro připojení z domova do sítě v práci. Použití VPN je také vhodné zvážit, pokud se často připojujete do cizích wi-fi sítí, kde může vaši komunikaci zachytávat i zcela cizí člověk, který je v dosahu sítě. VPN pak vlastně vytvoří bezpečný tunel, přes který můžete i ve veřejné wi-fi bez obav surfovat.

Bezpečné surfování

Dalším místem, kde se uplatňuje šifrování, jsou webové stránky. Stránku s šifrovaným přenosem dat poznáte podle toho, že začíná písmeny https, místo http. Kromě toho, že protokol https zajišťuje šifrování přenášených dat, umožňuje díky použití certifikátů také ověření, zda stránky, ke kterým se prohlížeč připojil, jsou opravdu těmi, za které se vydávají. S certifikáty a protokolem https se tedy setkáte na všech stránkách internetového bankovnictví, kde chrání díky šifrování vaše heslo před odposlechnutím případným útočníkem, ale také chrání uživatele, aby se nestali obětí například phishingového útoku. Dále se https používá všude tam, kde si prohlížeč a server vyměňují nějaké

citlivé informace, například jméno a heslo k e-mailové poště. Některé služby protokol https implicitně nepoužívají, což může být určité bezpečnostní riziko. Například u oblíbené služby Facebook je však možné v nastaveních použití https vynutit. Je potřeba si uvědomit, že váš prohlížeč důvěřuje automaticky všem certifikátům, které byly vydány některou z certifikačních autorit, jež máte v prohlížeči uvedeny jako důvěryhodné. Proto je potřeba zvýšené obezřetnosti při přidávání nových důvěryhodných certifikačních autorit. Některé servery, nabízející pornografické materiály nebo například cracky k hrám či jinému software uživatele často nutí právě k instalaci certifikátů pochybných certifikačních autorit. Dalším rozšířeným nešvarem v souvislosti s https a certifikáty je ignorování varovných hlášek prohlížeče, upozorňujících na to, že s certifikátem serveru není něco v pořádku. Mnoho uživatelů automaticky a bez přemýšlení odklikne pokračovat na webovou stránku, což může mít katastrofální následky. Pokud něco takového zaznamenáte při placení na e-shopu, při přístupu do on-line bankovnictví, či třeba do e-mailového účtu, doporučujeme dále nepokračovat a informovat o problému provozovatele služby jinou cestou, nejlépe telefonicky.