Vývoz šifer z USA

Strýček Sam nám nevěří?

16. září 1998 vydal Bílý dům tiskovou zprávu, podle níž dochází ke změně dosavadního zákazu vývozu silné kryptografie z USA. Vývoz šifrovacích technologií včetně SW podléhá schválení ministerstvem obchodu.

Dosud bylo (až na výjimky pro finanční sektor) prakticky povoleno vyvážet jen šifry s klíčem do 40 bitů. Protože ty jsou snadno rozluštitelné, vznikla řada iniciativ k vývozu silnějších šifer. Muselo být ovšem zajištěno, aby se vláda mohla v případě potřeby dostat k šifrovacím klíčům. A tak se zrodily systémy *Key Escrow* (systém sdílení klíčů), *Key Recovery* (systém obnovy klíčů) a letos *Operator Action* (klíče jsou v komunikačních zařízeních, zcela mimo kontrolu uživatele). Průmysl tato nepopulární opatření přijal jen s velkou nelibostí.

Vývoz šifer nově

Nová politika rozšiřuje vývozní sortiment a zjednodušuje licenční řízení. To nyní má záviset na kvalitě šifry, na státu, kam se vyváží, a na typu koncového zákazníka – sektoru.

Důležitou roli v něm hraje seznam 44 tzv. důvěryhodných států (ve vládním prohlášení je chybně uvedeno 45). V Evropě do něj patří Maďarsko, Polsko, Chorvatsko, Belgie, Rakousko, Dánsko, Finsko, Francie, Island, Irsko, Itálie, Lucembursko, Monako, Holandsko, Norsko, Portugalsko, Řecko, Spojené království, SRN, Španělsko, Švédsko, Švýcarsko a Turecko. Existuje i tzv. „seznam 41 států“, které tvoří oněch 44 bez Chorvatska, Hongkongu a Singapuru.

De iure a de facto

Protože neexistují prováděcí předpisy, zjišťovali jsme, jak bude postupováno nejen de iure, ale i de facto. Výsledkem jsou tato pravidla:

A. Žádná z následujících výjimek se netýká sedmi tzv. „teroristických“ států.

B. Bude zjednodušen vývoz 56bitové DES a ekvivalentních produktů (HW a SW), aniž by byl vyžadován systém Key Recovery.

C. Bude zjednodušen vývoz šifer s neomezenou délkou klíče bez systému Key Recovery pro tyto koncové uživatele:
1. pobočky amerických firem kdekoliv ve světě (pozn.: musí být ze 100 % vlastněny americkými občany) s výjimkou „teroristických států“;
2. pojišťovací společnosti a finanční instituce (včetně obchodníků s cennými papíry) – ale pouze ve 44 vyjmenovaných státech (výjimka


Countries Eligible to Receive General Purpose Encryption Commodities and Software Under License Exception

Argentina
Aruba
Australia
Austria
Bahamas
Barbados
Belgium
Brazil
Canada
Croatia*
Denmark
Dominica
Ecuador
Finland
France
Germany
Greece
Hong Kong*
Hungary
Iceland
Ireland
Italy
Japan
Kenya
Luxembourg
Monaco
Netherlands
New Zealand
Norway
Poland
Portugal
St. Kitts & Nevis
St. Vincent/Grenadines
Seychelles
Singapore*
Spain
Sweden
Switzerland
Trinidad & Tobago
Turkey
Uruguay
United Kingdom

Dokument, který způsobil tolik rozruchu.

platí i pro pobočky uvedených společností kdekoliv kromě „teroristických států“);
3. zdravotnické organizace (kromě vojenských a biochemických či farmaceutických výrobců) a online obchodníci (aplikace klient-server pro elektronické obchodování mezi klientem a obchodníkem, pokud se obchodování netýká zbraní a šifer) – ale pouze ve 44 vyjmenovaných státech (výjimka už neplatí pro pobočky uvedených společností).

D. Bude zjednodušen vývoz šifer s neomezenou délkou klíče se systémem Key Recovery pro ostatní firmy ze seznamu 41 států.

E. Ve všech ostatních případech se o udělení licence rozhoduje případ od případu, tj. jako dosud.

Proč nejsme důvěryhodní?

Podstata nové pozitivní změny je v bodech C2 a C3: Do určitých sektorů vybraných zemí je možné vyvážet kvalitní šifry bez průtahů. Našim médiím i mnoha firmám se samozřejmě nelíbí, že nejsme zařazeni do seznamu 44 států, jako je třeba Polsko, Maďarsko a Chorvatsko. Americká strana však k tomu nepodala žádné vysvětlení. Firmy, které by dotčený americký software k nám rády dovážely, se právem zlobí, že dovoz bude trvat déle a bude komplikován delším vývozním řízením (s nejistým výsledkem), zatímco u našich sousedů to bude jednodušší.

Tak to vidí i společnost SkyNet, která u nás začala prodávat PGP. Dokonce napsala otevřený dopis ministru průmyslu a obchodu Grégrovi, aby se zasadil o naše zařazení na onen seznam 44 „vyvolených“. Dobrá idea. Sice asi nebudeme jediným státem, který by si to přál, ale určitě má smysl se pídit po důvodech. Jistě by bylo dobré vědět, proč může USA vadit, že bychom měli ve finančních a zdravotnických institucích americký software s kvalitními šiframi. (Doufejme, že se záležitost brzy vysvětlí – proslýchá se totiž také, že naše vyřazení má na svědomí „šotek“, či lépe řečeno úředník, který dostal za úkol vyškrtnout z pracovní verze seznamu Cyprus a omylem při tom zrušil i následující položku Czech Republik... Nebyli jsme vlastně tím chybějícím čtyřicátým pátým státem?)

Podstata problému

Proč je vývoz šifer v USA postaven na roveň vývozu zbraní? Protože na odposlechové stanice a systémy, které obepínají celý svět, by silné šifry působily jako řízené střely na nepřátelské radary. Znemožnily by je. Jsou to opravdové zbraně, a zákon to tak také říká. Nezapomeňme na to!

Šifry jsou ovšem v mnoha podobách naprosto nezbytnou součástí moderních informačních systémů (šifrovaný přenos dat, autentizace, certifikáty, elektronický obchod, bezpečné weby, ...) a americký software měl dosud při zajišťování bezpečnostních funkcí v celé oblasti informačních technologií svázané ruce. Nemohl zcela volně používat kvalitní šifrovací nástroje, což způsobovalo miliardové obchodní ztráty. USA tedy musely najít kompromis mezi dvěma protichůdnými požadavky – nevyvážet „šifrovací zbraně“ znamená ohromné finanční ztráty, vyvážet je znamená riziko, že budou použity proti zájmům USA.

A co ochrana soukromí?

Místo všech úvah na toto téma nechme hovořit Barryho Steinhardta, prezidenta americké neziskové organizace Electronic Frontier Foundation bránící občanské svobody a soukromí. Řekl k tomu: *„... k přístupu jednotlivců k silnému šifrování a k ochraně našich soukromých komunikací to přispívá pramálo.“* Obstarožní 56bitové šifry je možné vyvážet kamkoliv, ale ty lepší jen do určitých průmyslových sektorů. Nejsou určeny pro občany.

Místo shrnutí dejme slovo jiné z významných osobností ve sféře informačních technologií. A. W. Cross, představitel IBM, se k nové iniciativě vyjádřil promptně a velmi přesně: *„Je to krok správným směrem. Myslím, že si uvědomují, že je tady ještě potřeba udělat hodně práce.“* A to je i pohled autora.

Na závěr bych chtěl poděkovat ing. Miroslavu Langovi z Microsoft Consulting Services Praha za cenné a upřesňující informace týkající se výkladu amerického vládního prohlášení.

Vlastimil Klíma (vklima@decros.cz)