

VÝVOZ ŠIFER Z USA

Strýček Sam už nám důvěřuje

19. říjen 2000 udělal ve vzájemných vztazích USA a ČR v oblasti šifer tečku za studenou válkou. Toho dne totiž vstoupil v platnost prováděcí předpis americké vlády k uvolnění exportu silné kryptografie. Pokud jde o vývoz silných šifer, které jsou v USA stále chápány jako zbraně, byli jsme tak už zařazeni k důvěryhodným zemím.

Novelizaci své politiky v oblasti šifrovacích systémů americká vláda zahájila už před třemi lety, stále se ale jednalo jen o malé změny. Dokonce ani členství ČR v NATO ještě v oblasti šifer neznamenal naše rovnoprávné postavení. Jak jsme vás informovali v březnovém čísle Chipu, v lednu t. r. došlo k velkému uvolnění tzv. retail produktů (viz infotypy). To mělo vliv například na implementaci silných šifer u tzv. krabicového softwaru. Zůstala ale oznamovací povinnost, tedy institut jednorázového posouzení a omezení na vývoz silných šifer pro vládní použití. To vše nyní padá. Oficiální text změn vydal k tomu zmocněný úřad ministerstva obchodu BXA (*U.S. Department of Commerce Bureau of Export Administration*) a je k dispozici na internetu (viz infotypy).

Třiadvacet vyvolených

Novelizace se týká exportu šifrovacích systémů do celkem 23 zemí. Američtí vývozcí tak mohou vyvázet veškeré šifrovací komodity a s nimi spojené technologie (kromě kryptoanalytických produktů) přímo do 15 členských zemí EU a dále do Austrálie, České republiky, Maďarska, Japonska, Norska, Polska, Švýcarska a na Nový Zéland bez vývozního povolení – přesněji řečeno na základě výjimky z vývozního povolení (exportní omezení pro ostatní země zůstávají v platnosti!). Firmy, organizace a úřady sídlící v těchto zemích nebo v Kanadě mohou vyvázet toto zboží do svých kanceláří nebo poboček po celém světě.

Zjednodušuje se i ohlašovací povinnost amerických distributorů, kteří mají své sídlo mimo americký kontinent (včetně poboček amerických firem), a ruší se ohlašovací povinnost po uskutečnění vývozu zařízení pro počítačové sítě a počítače s jediným procesorem (například osobní počítače, laptopy a handheldy), která jsou dodávána s předem zavedeným nebo obsaženým šifrovacím programovým vybavením.

O co jde

Dosah nové právní úpravy možná není na první pohled zcela patrný. Řekněme si proto alespoň stručně, jakých dalších produktů se zmíněná novelizace také dotýká.

Výrobky na bázi bezdrátových technologií

Produkty pro bezdrátovou technologii krátkého dosahu, které obsahují komponenty zajišťující kryptografické funkce, mohou být dodávány jakémukoliv koncovému uživateli bez vývozního povolení, technického posouzení a oznamovací povinnosti. Patří sem například zařízení

na reprodukci zvuku, kamery, videorekordéry, příslušenství k osobním počítačům, ruční zařízení, mobilní telefony, ledničky, pračky a mikrovlnné trouby, které spolu komunikují pomocí bezdrátových technologií krátkého dosahu.

Otevřená kryptografická rozhraní

Dosud nebylo možné vyvázet výrobky obsahující tzv. otevřené kryptografické rozhraní, které umožňuje do softwarového balíku nebo firmwaru instalovat vlastní šifry. Nyní ano. Umožní to například dovážet hardware nebo software a poté do něho implementovat národní šifry. Příslušné národní nástroje, které se tak včlení do originálního výrobku, je možné digitálně podepsat americkým výrobcem na základě výjimky z vývozního povolení a bez posouzení takového zahraničního výrobku.

Zdrojové kryptografické kódy

Zdrojový kód, který se nepokládá za veřejně dostupný, může být nyní vyvážen přímo na základě výjimky z vývozního povolení koncovým uživatelům, jimiž ale **nesmějí být vládní úřady** (jak vidíte, ještě tu nějaký háček je) a zůstává také povinnost požádat o klasifikaci u BXA. Dále se zpřesňuje způsob nakládání s objektovým kódem, který byl kompilován na základě veřejného zdrojového kódu. (Poznamenejme, že zdrojový kód, který je veřejně dostupný, je možné vyvázet bez omezení už podle předchozí novely.)

Závěr

Přes padesát let trvající zákazy byly zrušeny. V České republice je ale pochopitelně ještě mnoho úřadů, organizací i jednotlivců používajících slabé šifry v americkém softwaru a výrobcích. Situace na trhu se ovšem nyní bude zlepšovat a dojde k širokému používání silných šifer. Týká se to nejen oblastí osobních počítačů, ale i telekomunikací a dalších odvětví. Lépe bude zabezpečen i elektronický obchod a rozšíří se nabídka nástrojů pro elektronický podpis. | | | *Vlastimil Klíma (v.klima@decros.cz)*

infotypy

Oficiální oznámení úřadu BXA:

► <http://www.bxa.doc.gov/Encryption/19Oct2KFactsheet.html>

Obsah předchozího uvolnění:

V. Klíma: Konečně!, Chip 3/00, str. 40 – 41, elektronicky též na
► www.decros.cz/Security_Division/Crypto_Research/archiv.htm