UVOLNĚNÍ SILNÝCH ŠIFER

Konečně!

Nový rok přinesl i dlouho očekávané uvolnění v oblasti vývozu silných šifer z USA. Přes padesát let trvající zákazy byly překonány a nastartovaly se tak změny vynucené rozvojem informační společnosti.

Nová opatření budou mít ohromný vliv na americké výrobce softwaru i hardwaru a tím také na průmysl informačních technologií na celém světě. Díky globalizaci, internetu a elektronickému obchodu pocítíme novou informační politiku i u nás. Počítačový svět bude o něco bezpečnější. Společně s připravovaným americkým šifrovacím standardem AES, o kterém vás budeme v nejbližší době informovat, to uspíší stav, kdy se silné šifry konečně stanou dostupnými běžným uživatelům k ochraně soukromí i majetku bez zbytečných průtahů.

INFORMAČNÍ ODZBROJENÍ

Šifry i šifrovací programy a zařízení byly donedávna v USA i jinde považovány za zbraně a jejich export podléhal stejným omezením jako třeba vývoz granátů. Něco takového bylo v informačních technologiích, kde data znamenají často i velké peníze, silnou brzdou pokroku. Nicméně zákon je zákon, a tak se do běžného komerčního softwaru, který šel z USA do celého světa (Microsoft, Novell, Lotus...), musely zavádět tzv. slabé šifry, luštitelné s určitými, ale ne velkými investicemi. Naproti tomu na území USA mohly být používány šifry silné, což nakonec vedlo k výrobě dvojího softwaru. To se samozřejmě prodražovalo a kompatibilita byla ta tam.

PRODEJ WINDOWS 2000 OBSAHUJÍCÍCH 128BITOVÉ ŠIFROVÁNÍ NEMÁ BÝT NIJAK OMEZEN.

Některé společnosti od tohoto řešení sice ustoupily, pohrobci slabých šifer ale zůstali v mnoha operačních systémech a činí je dodnes oslabenými. Doufejme, že během několika let se tyto „díry“ zacelí a dojde k celkovému zvýšení bezpečnosti nejen při odesílání zašifrovaných a digitálně podepsaných e-mailů, ale i k ochraně dat vlastními nástroji operačních systémů.

Z uvedených důvodů přicházeli američtí výrobci o světový trh s bezpečnostními službami a jejich místo obsadily zahraniční společnosti. Nakonec to byla právě lobby informačních technologií, která nové změny za asistence vlivných politiků prosadila. Prezident Clinton je sice zaobalil do celkového kontextu nové bezpečnostní politiky (docela zajímavý širokospektrální dokument, viz infotipy), ale zainteresovaní vědí, že to byl výsledek deset let trvajícího úsilí velkých informačních společností.

Změny byly předběžně ohlášeny už v září minulého roku, ale ne všichni věřili, že pouhá politická deklarace bude mít prakticky užitečnou realizaci. Očekávalo se opět, že podstata bude skryta v detailech právnických formulací („the devil is in details“) tak, jako tomu bylo ve třech předchozích případech, kdy „uvolnění restrikcí“ přineslo koncepty „key escrow“, „key recovery“ a další, kamuflující skutečnost, že silné šifry je sice možné vyvážet, ale tajná služba stejně musí mít možnost se k nim dostat. Dnes je situace jiná, i když podle amerických demokratických institucí stále ne taková, jak by samy chtěly, tj. naprosto bez omezení.

Čtrnáctého ledna 2000 tak vstoupila v platnost nová opatření týkající se exportu šifrovacích zařízení. Vydal je k tomu zmocněný úřad ministerstva obchodu BXA *(U.S. Department of*

Commerce Bureau of Export Administration) a oficiální text zveřejnil na internetu (viz infotipy). Zároveň byla vyhlášena 120denní lhůta k připomínkám a předpokládá se, že do šesti měsíců bude možné na základě veřejné diskuse učinit ještě technické úpravy.

Co je nového

Stručně řečeno, nová opatření definují:

- sedm států (T7) „podporujících terorismus“, pro něž platí i nadále dosavadní přísná omezení (Irák, Írán, Kuba, Libye, Severní Korea, Súdán, Sýrie a také část Afghánistánu);
- tzv. „retail“ a „mass“ produkty (například komerční „krabicový software“), kde bude možný téměř neomezený prodej, a to jak co do kvality šifer, tak vzhledem ke koncovému uživateli (vyjma T7);

UVOLNĚNÍ VÝVOZU SILNÝCH ŠIFER Z USA JE VÝSLEDKEM DLOUHOLETÉHO TLAKU SPOLEČNOSTÍ PŮSOBÍCÍCH NA POLI INFORMAČNÍCH TECHNOLOGIÍ.

- určité restrikce pro prodej vládním organizacím (zde se ale jedná zejména o potřeby ozbrojených sil, nikoli o potřeby „správních“ systémů);
- velmi benevolentní podmínky pro export zdrojových kódů šifer (tj. nepřeložených a přímo nespustitelných programů), a tedy například i pro jejich publikování na internetu;
- institut *jednorázového technického posouzení* (technical review), *podávání zpráv o prodeji* a několik typů *vývozních licencí* (ENC, TSU, KMI, ELA, IL apod.) pro „složitější“ případy.

Jak je vidět, v detailech přece jen zůstal ukryt citovaný ďáblík. Sami Američané, a to včetně velkých společností, které mají svá právní oddělení, zkoumají, co vlastně je povoleno a co není. Kritizují zejména složitost opatření. Proto bohužel také není v silách tohoto článku rozpitvat všechny souvislosti a i v USA samých se všeobecně čeká na precedenty a reakce předních společností informačních technologií (či spíše jejich právníků).

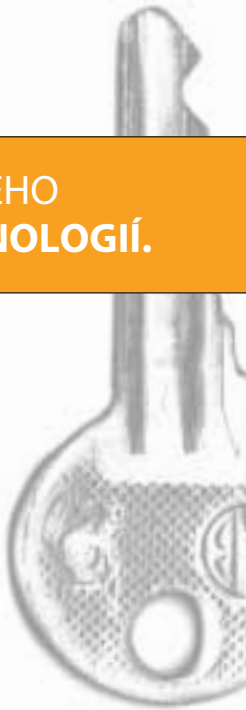
Muselo to přijít

Někteří nadšenci však nečekají a už udělali riskantní kroky. Například 63letý John Young, známý v kryptografickém společenství, zveřejnil vykonatelný kód programu PGP na své webové stránce (viz infotipy), Philip Zimmermann si zase splnil svůj sen a s mírným vzrušením odeslal svůj první kvalitně šifrovaný e-mail přes hranice USA. Aby to bylo dostatečně pikantní, adresoval ho na ministerstvo obrany do Anglie, a to za účasti kongresmanů Lofgrena a Goodlatta, propagátorů nových opatření.

Pro zrušení restrikcí vykonal kus práce i William Crowell jako předseda prezidentské komise pro vývoz šifer. Zajímavé přitom je, že býval zástupcem ředitele NSA, tajné služby, která stála 50 let v pozadí za těmito restrikcemi. V současné době je ale prezidentem jedné velké společnosti vyrábějící šifrovací zařízení. Je zřejmé, že díky jeho minulé pozici mu v komisi těžko někdo mohl vytírat oči „národně bezpečnostními argumenty“.

Že situace nazrávala, snad dokumentuje i následující příklad. Ještě několik měsíců před vyhlášením těchto opatření jeden šestnáctiletý Američan zpřístupnil na webu zdrojové kódy své silné šifry. A nejen to, veřejně to oznámil s vědomím, že je to trestné, ale poznamenal: „Ať si zkusí kvůli tomu zavřít dítě!“

Jedna z prvních reakcí velkých společností po ohlášení nových opatření přišla od Microsoftu. Bylo oznámeno, že operační systém Windows 2000, který se bude po celém světě prodávat podle nových exportních opatření, bude mít už implementováno 128bitové šifrování. Prodej Windows 2000 by neměl být nijak omezen a měl by být zahájen během února (viz infotipy). Další kroky velkých výrobců budou jistě následovat a za několik měsíců to už nebude nic nového. A tak by to také mělo být.



Závěr

Společnosti i lidé, kteří byli po léta exportními omezeními na silnou kryptografii poškozováni nebo dokonce trestně stíháni, mají důvod k oslavám. Připojme se k nim, neboť je to krok správným směrem. Doufejme také, že nastartované změny vytvoří takový tlak, aby byla zrušena i zbývající nesmyslná opatření. Jde totiž o budoucnost nejnadějnějších odvětví – informačních technologií a telekomunikací. Zaručení jejich bezpečnosti umožní nejen rozvoj současných, ale zejména vznik nových služeb, v nichž dosud nebylo možné použít silné nástroje na ochranu dat.

Vlastimil Klíma | v.klima@decros.cz

infotipy

- **Dokument „Národní bezpečnostní strategie v novém století“**
  http://cryptome.org/nss2000.htm
- **Plný text oficiálního dokumentu o nových vývozních omezeních**
  http://www.epic.org/crypto/export_controls/regs_1_00.html
- **Odpovědi BXA na dotazy**
  http://www.columbia.edu/~ariel/jlewis-anwers.html
- **Nová šifrovací politika**
  http://www.bxa.doc.gov/Encryption/qanda.html
- **Typy vývozních licencí a průvodce pro vyplnění žádostí**
  http://www.bxa.doc.gov/Encryption/licchart.html
  http://www.bxa.doc.gov/Encryption/guidance.html
- **Prohlášení Microsoftu**
  http://biz.yahoo.com/prnews/000118/wa_microso_1.html
- **Web Johna Younga s PGPfreeware 6.5.2a pro Windows 9x/NT/2000**
  http://cryptome.org/pgpfree/PGPfreeware_6_5_2a.zip