Nový čínský zákon o šifrování dat o kybernetické bezpečnosti

- CZ24 News | 16. února 2020

- Poté, co budou všechna tato pravidla týkající se *"kybernetické bezpečnosti"* uvedena v platnost, nebude moci žádná zahraniční společnost šifrovat data tak, aby je čínská ústřední vláda a Komunistická strana Číny nemohly přečíst. Jinými slovy, firmy budou muset čínským úřadům dát k dispozici své šifrovací klíče.
- Čínští úředníci budou moci podle čínských zákonů sdílet získané informace s čínskými státními podniky a ty budou moci tyto informace použít proti své zahraniční konkurenci.

1. ledna 2020 vstoupil v platnost čínský zákon o šifrování dat (kryptografii). Tento právní předpis navazuje na implementaci víceúrovňového systému ochrany 2.0 z 1. prosince 2019, vydaného na základě zákona o kybernetické bezpečnosti z roku 2016.

Tato opatření ukazují nekompromisní rozhodnutí Pekingu zabavit zahraničním společnostem veškerou jejich komunikaci, data a další informace uložené v elektronické podobě v Číně.

Prezident Trump by měl využít své pravomoci, které má pro případ nouze, a měl by americkým společnostem zakázat tato nová pravidla dodržovat a ukládat data v Číně.

Poté, co budou všechna tato pravidla týkající se *"kybernetické bezpečnosti"* uvedena v platnost, nebude moci žádná zahraniční společnost šifrovat data tak, aby je čínská ústřední vláda a Komunistická strana Čbezíny nemohly přečíst. Jinými slovy, firmy budou muset čínským úřadům dát k dispozici své šifrovací klíče.

Společnostem bude rovněž zakázáno používat virtuální privátní sítě (VPN) pro zachování utajení dat a někteří pozorovatelé se domnívají, že společnosti již nebudou moci používat ani soukromé servery.

Jakmile bude pekingský systém zaveden, bude tak invazivní, že čínské orgány již nebudou muset žádat zahraniční společnosti o poskytnutí dat. Čínští úředníci si budou moci tato data jednoduše stáhnout sami.

Steve Dickinson na blogu *China Law Blog* napsal: *"Jakmile jakákoliv data překročí čínskou hranici, tak budou dostupná čínské vládě a Komunistické straně Číny."*

Schopnost Pekingu nahlížet do počítačových sítí zahraničních společností bude mít velmi negativní důsledky, poznamenal Dickinson. Zaprvé, čínští úředníci budou moci podle čínských zákonů sdílet získané informace s čínskými státními podniky a ty budou moci tyto informace použít proti své zahraniční konkurenci.

Za druhé, tato nová čínská pravidla povedou téměř jistě k tomu, že zahraniční společnosti ztratí po celém světě ochranu svých obchodních tajemství. Zveřejněním ztrácejí obchodní tajemství svůj status. Jakmile společnost dovolí, aby bylo její obchodní tajemství přenášeno na její počítačové síti v Číně, musí předpokládat, že se jej dozví Peking. Podle Dickinsona: *"Od teď už žádná společnost nemůže předpokládat, že její obchodní tajemství zůstanou tajemstvím i poté, co se dostanou do Číny prostřednictvím Číňany kontrolované počítačové sítě. Společnostem hrozí, že ochrana jejich obchodních tajemství zmizí i mimo Čínu."*

Za třetí, čínský program kybernetické bezpečnosti vystavuje společnosti postihům za porušení

právních předpisů USA týkajících se vývozu technologií. Americké společnosti předpokládají, že technologie, na kterou se vztahuje zákaz vývozu ze strany USA, není *"vyvezena"*, pokud je uchovávána v čínské počítačové síti chráněné koncovým šifrováním (*end-to-end*), jinými slovy, že není k dispozici čínským orgánům. Protože však společnostem již nebude dovoleno koncově šifrovat data, bude uložení dat v Číně téměř jistě považováno za porušení amerických právních předpisů pro vývoz technologií.

Tato čínská opatření z 1. prosince 2019 ovšem neznepokojují všechny analytiky. Například James Andrew Lewis tvrdí, že nová pravidla Pekingu jsou *"legitimní snahou"* o zabezpečení počítačových sítí v Číně. Navíc tvrdí, že Číňané nepotřebují nová pravidla víceúrovňového systému ochrany 2.0 (MLPS 2.0) k získávání informací, protože se svými pokročilými hackerskými skupinami *"APT"* mohou ukrást cokoliv, se jim zamane. *"Jejich záměrem není škodit,"* tvrdí Lewis s odkazem na čínské úředníky.

Není jasné, jak Lewis, technický expert Centra pro strategická a mezinárodní studia (*Center for Strategic and International Studies,* CSIS) se sídlem ve Washingtonu, D.C., může vědět, co mají čínští úředníci za lubem. Kromě toho, popsat tento záměr Číny jako neškodný se zdá být naivní – ba dokonce směšné – vzhledem k tomu, že Čína každý rok ukradne americké duševní vlastnictví v hodnotě stovek miliard dolarů a čínský vládce Si Ťin-pching odhodlaně pokračuje ve svých rozhodných útocích na zahraniční společnosti. Za těchto okolností tedy musíme předpokládat, že čínští úředníci nemají čisté úmysly.

Lewis také zlehčuje jednu podstatnou věc, a tou je to, že jakmile budou mít čínští kybernetičtí špióni šifrovací klíče a přístup k čínské počítačové síti zahraniční firmy, budou schopni snadněji proniknout i do počítačových sítí této firmy mimo Čínu. Bude tedy jen otázkou času, než Peking ukradne data a konkurenční společnosti zničí tak, že se stanou lehkou kořistí čínských společností. Mnoho lidí tvrdí, že Čína ukradla data kanadské společnosti Nortel Networks Corporation, a tato firma v důsledku toho již téměř před deseti lety zbankrotovala. Podle novin *Financial Post* byla zmíněná společnost hackery *"rozcupována na kousky"*.

A konečně, Lewis z CSIS si odmítá připustit, že pekingský zákon z 1. prosince 2019 obecně oficiálně uzákoňuje regulační a informační dohled Číny – jinými slovy řečeno čínskou krádež.

Senátor Josh Hawley je k záměrům Pekingu oprávněně nedůvěřivý. V listopadu 2019 představil tento republikán ze státu Missouri návrh zákona o národní bezpečnosti a ochraně dat (*National Security and Data Protection Act of 2019*), který by americkým společnostem zakázal ukládat uživatelská data a šifrovací klíče v Číně. Americké technologické společností podnikající v Číně se přijetí tohoto zákona samozřejmě brání.

Přesto však existuje někdo, kdo by mohl Hawleyův zákon účinně implementovat pouhým škrtem pera. Prezident Donald John Trump může využít své široké pravomoci vyplývající ze zákona o mimořádných ekonomických pravomocech (*International Emergency Economic Powers Act*) z roku 1977, který americkým společnostem zakazuje, aby dodržovaly pro ně destruktivní nová pravidla vztahující se na ukládání jejich dat v Číně.

Důvodem takového rozsáhlého prezidentského nařízení je to, že je v zájmu občanů USA, aby Čína nepřevzala kontrolu nad americkými společnostmi podnikajícími v Číně – což bude pravděpodobně důsledkem uplatňování zákonů platných od 1. prosince 2019 a 1. ledna 2020.

Tento mimořádný prezidentský dekret by zřejmě prakticky vytlačil americké společnosti z Číny, byl by to tedy velmi drastický krok. Přesto je to právě Čína, která má v úmyslu zavést neuvěřitelně ambiciózní (čti drzé) získávání dat a nutí tak USA k řešení tohoto problému.

Ochrana amerických dat je v zásadním zájmu občanů USA. Prezident Trump by měl tento dekret neprodleně vydat.

Gordon G. Chang je autor knihy *“Přicházející kolaps Číny”*