

Pamatujete rok 2009? Tehdy reprezentanta Strany Zelených - Kateřina Jackues nevěděla, co je biomasa. Považovala ji za mrkev. Jinými slovy za Zelené tlačila nějaké koncepty, které vůbec nechápala a nerozuměla jim. Ale Zelená tehdy frčela a marketing fungoval.

Stejná situace nastala nyní u Pirátů. Viz. nápad místopředsedkyně Pirátů, že hackingu Číny zabrání kontrola výroby součástek v Čínských továrnách - viz <https://www.novinky.cz/domaci/494308-recept-piratu-proti-cinskemu-hackingu-musime-koukat-jak-vyrabeji-soucastky.html>. Jedná se o reakci na to, že síťové prvky Huawei mají zřejmě backdoory a představují bezpečnostní riziko.

Citujme z článku „Musíme mít kontrolu nad tím, z jakých komponent se kritická infrastruktura skládá. Je to úplně jednoduché. Musí to být vyráběné v důvěryhodných továrnách. Musí být kompletní dokumentace, o tom, co jaké prvky dělají,“ řekla Richterová v pořadu Otázky Václava Moravce."

Takže si asi paní místoředsedkyně odborníků na IT představuje, že tam ty "zadní vrátka" přestanou montovat. Asi najde sklad zadních vrátek a sebere jim klíč. Nebo bude koukat, zda se tam nenapájel kus křemíku navíc na nějakou tištěnou desku... Určitě tomu rozumí, takže pozná, že ten který čip je ten mega problém.

Jenom pro vysvětlení - jak telefon, tak síťový prvek v telekomunikační infrastruktuře je bez obslužného software k ničemu. Stejně tak váš notebook, nebo stolní počítač. Největší rizika se pojí právě s obslužným softwarem. Když vynecháme např. špatnou architekturu čipů Intelu, která byla zabudována již na úrovni návrhu, resp. návrh byl výkonný, ale ne bezpečný, tak je iluzorní představa, že Číňané mají největší díry v HW návrhu.

Problémy jsou obvykle zakopané v detailu, v kusu kódu, který dělá navíc něco, co by neměl a provozovatel nemá možnosti a kapacity takový problematický kód nalézt a prověřit. Další věc je, že se tato řešení servisují vzdáleně, přes VNP, atd... Nikdo není schopen bez toho, aniž by si ty obslužné SW napsal sám, co v tom vše je. Dnes se dá podstrčit špatný software na úrovni

ovladače řadiče pevného disku, takže jestli to v továrně pájí tak, nebo onak, je úplně, ale úplně jedno.

Takže ano, Čínané pravděpodobně mají softwarové backdoory v dodávaných řešeních. Stejně tak jako je mají Američané. Co chvíli se ukáže, že velká americká společnost pochopitelně spolupracuje s USA vládou a vydá jí, co potřebuje. A to i z cloudových řešení. A když se cuká, využívají zpravodajské služby různých backdoorů, o kterých ví pár vyvolených. Bavíme se o milionech řádků zdrojového kódu, kdo má k němu přístup, dále čas, kapacity a znalosti to celé projít a říci, že to jenom orá, ale už neseje?

A co se týče nás, pokud jsme jako EU, nejenom Česká republika, sklouzli do situace, kdy se tu prakticky nic klíčových IT komponent fyzicky nevyrábí, software se píše v Asii a vedení státu nemá nejmenší představu o bezpečnosti, tak nezbývá, než počítat s tím, že co napíšete, pošlete, uložíte, nejenom u sebe, ale i na internetu, si mohou přečíst jak v Číně, tak v USA.

{comments on}