ZNALECKÝ POSUDEK Č. 1483/2016

ODBORNÉ VYJÁDŘENÍ K USTANOVENÍ § 82 ODST. 1 ZÁKONA Č. 186/2016 SB., O HAZARDNÍCH HRÁCH

Zpracoval:

ING. JAN FANTA, CISA, CRISC

Kolínská 14, 130 00 Praha 3

soudní znalec v oborech ekonomika, elektronika, kybernetika, výpočetní technika

certifikovaný auditor informačních systémů

certifikovaný v IS risk managementu

ZNALECKÝ POSUDEK

Na základě žádosti advokátní kanceláře Weinhold Legal, v. o. s., Na Florenci 15, 110 00 Praha 1 ze dne 8. srpna 2016, jsem se ujal zpracování odborného znaleckého vyjádření k ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách (dále také „Zákon").

1 Otázky na znalce

1. Jaké osoby lze z Vašeho odborného pohledu ve vztahu k ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách v platném znění označit za poskytovatele připojení k internetu, respektive za poskytovatele připojení k internetu na území České republiky, jak tyto pojmy používá ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách, v platném znění?

2. Jak z Vašeho odborného pohledu chápete pojem internetová stránka ve vztahu k ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách v platném znění, jak tento používá ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách, v platném znění?

3. Je technicky proveditelné zamezit v přístupu k internetovým stránkám, jak vyžaduje ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách, v platném znění a zároveň tak zajistit aby nebyly omezeny další poskytované a běžně využívané služby (e-mail, přenos souborů protokolem FTP atd.)?

4. Jaká konkrétní technická opatření by bylo nezbytné přijmout v rámci plnění povinnosti zamezit v přístupu k internetovým stránkám ve smyslu ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách, v platném znění?

5. Jaké by dle Vašeho odborného odhadu byly náklady na zavedení opatření pro zamezení v přístupu k internetovým stránkám, která jste vymezil v odpovědi na otázku č. 4?

6. Bylo by možné zamezení v přístupu k internetovým stránkám ve smyslu ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách, v platném znění, provést technicky či ekonomicky efektivněji, než jak vyžaduje odkazované zákonné ustanovení?

7. Existuje možnost hraní internetové hazardní hry bez použití internetových stránek?

2 Analytická část

2.1 Analýza § 82 zákona č. 186/2016 Sb.

2.1.1 Ustanovení paragrafu 82 Zákona – Blokace nepovolených internetových her

(1) Poskytovatelé připojení k internetu na území České republiky jsou povinni zamezit v přístupu k internetovým stránkám uvedeným na seznamu internetových stránek s nepovolenými internetovými hrami (dále jen „seznam nepovolených internetových her").

(2) Na seznam nepovolených internetových her se zapíše internetová stránka, na níž je provozovaná internetová hra v rozporu s § 7 odst. 2 písm. b).

(3) Povinnost podle odstavce 1 jsou poskytovatelé připojení k internetu povinni splnit ve lhůtě 15 dní ode dne zveřejnění internetové stránky v seznamu nepovolených internetových her.

2.1.2 Analýza § 82 zákona č. 186/2016 Sb. z hlediska odbornosti znalce

Znalec, tak aby splnil zadání zadavatele, se ve svém odborném vyjádření bude zabývat i rozborem odborných technických výrazů v tomto paragrafu použitých. Soustředí se ale výhradně na ty, které spadají do jeho odbornosti. Pro splnění zadání bude nutné tyto výrazy

identifikovat a popsat tak, aby i pro neodborníka byly tyto výrazy jasné, jednoznačné a pochopitelné.

Jedná se o tyto výrazy:

a. Poskytovatel připojení k internetu;
b. Internet;
c. Internetová stránka.

Tyto a další výrazy jsou obsáhle a podrobněji vysvětlené v kapitole 2.3.

2.2 Analýza otázek kladených na znalce

Znění paragrafu 82 Zákona používá řadu technických výrazů ve spojení s jeho ustanoveními. Vzhledem ke skutečnosti, že moderní technologie umožňující použití celosvětového systému propojených počítačových sítí jsou dnes dostupné té nejširší i laické veřejnosti, stává se velice často, že tyto jejich výrazy jsou nesprávně nebo nepřesně používány. Jedná se o běžné použití výrazů, dříve používaných pouze odborníky, nyní rozšířených mezi laickou veřejnost. K tomu přispívá i četnost jejich používání v médiích a celosvětovou propojeností médií, sociálních sítí a z tohoto důvodu pak i používání zkratkovitých výrazů (like, klik apod.). To vše ve výsledku vede k posouvání významu těchto výrazů, jejich rozdílnému chápání různými skupinami lidí a potenciálně tedy i k nedorozuměním z toho plynoucích. Tento trend znalec zde jen konstatuje, rozbor tohoto trendu nepatří do znalcovy odbornosti.

Otázky 1 a 2 jsou zaměřeny přímo na zpřesnění použité terminologie pro zvýšení srozumitelnosti jednotlivých výrazů v Zákoně použitých.

Otázky 3, 4, 6 a 7 se pak věnují možným technickým opatřením vyžadovaných ustanovením § 82 Zákona a otázka 5 směřuje k odhadům nákladů na zavedení těchto technických opatření.

2.3 Vysvětlení terminologie použité v posouzení

- **Autonomní systémy korporátních společností** – konektivita mimo ČR. Celá řada velkých (nejen nadnárodních) korporací používá vlastní autonomní systémy elektronické komunikace. Tyto využívají pro připojení do svých sítí „tunely", většinou VPN. Kromě toho jejich systémy umožňují připojení na internet pro uživatele svých systémů. Poskytují tedy připojení k internetu pro území České republiky, ale jejich připojení nemusí být realizované prostřednictvím poskytovatele na území České republiky.
- **DNS** (Domain Name System) je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si tyto servery vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě. DNS poskytuje lidem možnost pracovat na internetu s doménovými jmény, která jsou pro lidi dobře zapamatovatelná a pochopitelná, zatímco stroje pracují s překladem doménových jmen na IP adresy.
- **Hotspot** (v terminologii internetu) místo či oblast s možností bezdrátového připojení k internetu.
- **HTTP** (Hypertext Transfer Protocol) je internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML. Tento protokol je tím nejvíce používaným a zasloužil se o obrovský rozmach internetu v posledních letech. V současné době je používán i pro přenos dalších informací. HTTP používá jako některé další aplikace tzv. jednotný lokátor prostředků (URL, Uniform Resource Locator), který specifikuje jednoznačné umístění nějakého zdroje v internetu. Samotný protokol HTTP neumožňuje šifrování ani zabezpečení integrity dat.
- **HTTPS** (Hypertext Transfer Protocol Secure) je v informatice nadstavba síťového protokolu HTTP, která umožňuje zabezpečit spojení mezi klientem (např. webovým

prohlížečem) a serverem před odposloucháváním, podvržením dat a umožňuje též ověřit identitu protistrany. HTTPS používá protokol HTTP, přičemž přenášená data jsou šifrována. Podíl HTTPS v posledních letech rychle roste, stává se postupně standardem. Důvěryhodné subjekty poskytující služby prostřednictvím svých webových stránek komunikují s klientem prostřednictvím HTTPS. Tato nadstavba není nijak finančně ani technicky náročná.

- **Internet** je velmi zjednodušený název pro celosvětovou otevřenou a veřejnou síť propojující zdroje aplikací, informačních aktiv a komunikačních prostředků umístěných na serverech. Internet je celosvětový systém propojených počítačových sítí („síť sítí"), ve kterých mezi sebou počítače komunikují pomocí rodiny protokolů TCP/IP. Společným cílem všech lidí využívajících internet je bezproblémová a necenzurovaná komunikace (výměna dat). Nejznámější službou poskytovanou v rámci internetu je World Wide Web (www), tedy webové stránky obsahující kombinace textu, grafiky a multimédií propojených hypertextovými odkazy a e-mail (elektronická pošta), avšak nalezneme v něm i desítky dalších. Laici někdy spojují pojmy www a internet, i když www je jen jednou z mnoha služeb, které je na internetu možné nalézt.
- **Internetová doména** (doménové jméno) je v informatice označení jednoznačného jména (identifikátoru) počítače nebo počítačové sítě, které jsou připojené do internetu. Příkladem doménového jména je zápis www.seznam.cz.
- **IP adresa** je v informatice číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol).
- **Paket** označuje v informatice jistý blok dat přenášený v počítačových sítích. Lze ho chápat jako balíček s přenášenými daty obsahující též řadu řídících dat určených pro obsluhu přenosu.
- **Podnikatelé mimo oblast poskytování elektronických komunikací**. Řada zmíněných autonomních systémů jsou poskytovatelé komunikačních služeb, kteří ale nespadají do oblasti poskytování elektronických komunikací.[1]
- **Proxy server** je zařízení, které funguje jako prostředník mezi klientem (uživatelem) a cílovým počítačem (serverem), překládá klientské požadavky a vůči cílovému počítači vystupuje jako sám klient. Používá se na mnoho funkcí při řízení a kontrole provozu a chování klientů (uživatelů). Pro účely tohoto posudku se proxy serverem rozumí jedno z mnoha možných použití tohoto pojmu, a to jako filtrovací proxy server. Jsou to servery filtrující obsah komunikace a umožňující kontrolu a řízení obsahu v jednom nebo obou směrech přes tento server. Běžně se pro tyto účely používá v komerčních i nekomerčních organizacích pro kontrolu a filtrování využívaní internetového připojení pro povolené účely
- **URL**, celým názvem Uniform Resource Locator („jednotná adresa zdroje") je řetězec znaků s definovanou strukturou, který slouží k přesné specifikaci umístění zdrojů informací (ve smyslu dokument nebo služba) na internetu. URL definuje doménovou adresu serveru, umístění zdroje na serveru a protokol, kterým je možné ke zdroji přistupovat.
- **Virtuální privátní síť** (zkratka VPN, anglicky virtual private network) je v informatice prostředek k propojení několika počítačů prostřednictvím (veřejné) nedůvěryhodné počítačové sítě. Lze tak snadno dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní

---

[1] Pro účely tohoto vyjádření dostatečná informace, pro přesné definice znalec odkazuje na znění Zákona o elektronických komunikacích 127/2005 Sb., viz zejména §7 a násl. a §38 - §40.

(a tedy důvěryhodné) sítě. Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů, dojde k autentizaci, veškerá komunikace je šifrována, a proto můžeme takové propojení považovat za bezpečné.

- **Webhosting (také web hosting)** je pronájem prostoru pro webové stránky na cizím serveru. Pronajímatel serveru bývá označován jako poskytovatel webhostingu.
- **Webová stránka** je dokument, který je možné pomocí webového prohlížeče zobrazit na displeji počítače. Webové stránky jsou obvykle poskytované v rámci World Wide Webu. Stránky se skládají z textu, multimediálních dat (obrázky, videa, zvuky, vložené objekty (další stránky) a odkazů, které umožňují přechod na další webové stránky. Webová stránka se pak může sestávat z jedné stránky nebo z dalších stránek, zřetězených bez omezení jejich počtu a úrovní. Tyto stránky pak nemusí mít vůbec vztah vzájemné funkcionality, takže na jedné stránce v řetězu může být zcela jiná funkcionalita. Blokace stránky pak znamená blokaci dalších funkcí webové stránky. Webové stránky mohou být uloženy v podobě souborů na pevném disku nebo je poskytují webové servery prostřednictvím počítačové sítě nebo internetu, kde jsou přenášeny pomocí protokolu HTTP anebo šifrovaného HTTPS. Stránky mohou být statické (obsahují stále stejný obsah, jsou uloženy v souborech) nebo dynamické (mění svůj obsah v čase, vytváří je program na straně webového serveru, například i pouhou formou dotazu uživatele).
- **Webový prohlížeč** (též browser) je v informatice označení pro počítačový program, který slouží pro prohlížení webových stránek. Webový prohlížeč dle pokynů uživatele (kliknutí na odkaz, zadání URL adresy) komunikuje pomocí HTTP protokolu s webovým serverem a přijatá data pomocí obsažených značek zformátuje a zobrazí na obrazovce počítače. Textové prohlížeče zobrazují stránky jako text, obvykle velmi jednoduše formátovaný. Grafické prohlížeče umožňují složitější formátování stránky včetně zobrazení obrázků. Mezi nejznámější grafické webové prohlížeče patří Google Chrome, Internet Explorer, Mozilla Firefox, Safari, Opera, Maxthon a další. Mezi textové pak Links, Lynx a další.
- **Webový prohlížeč Tor**. Webové prohlížeče běžně dokáží zajistit uživateli anonymitu pohybu na internetu (nelze zjistit, kdo a odkud přistupuje k na dané URL) a také zpřístupnit webové stránky, které jsou v zemi uživatele blokované. Mezi takové webové prohlížeče patří například Tor Browser, Opera Tor nebo xB Browser (upravený Firefox), pro účely tohoto posudku je dále označuji jako Webové prohlížeče Tor.
- **Wi-Fi.** Cílem Wi-Fi sítí je zajišťovat vzájemné bezdrátové propojení přenosných zařízení a dále jejich připojování na lokální (např. firemní) sítě. Je používaná k bezdrátovému připojení do sítě internet v rámci rozsáhlejších lokalit a tzv. hotspotů (přístupových bodů). Wi-Fi zařízení jsou dnes prakticky ve všech přenosných počítačích a i v některých mobilních telefonech.

3 Odborné vyjádření znalce k zadané problematice

3.1 Vysvětlení systému internetu

Internet je globální systém propojených počítačových sítí, které propojují miliardy různých zařízení na celém světě. Jedná se o síť sítí, která se skládá z milionů soukromých, veřejných, akademických, obchodních a vládních sítí místních i celosvětových. Tato zařízení a sítě jsou propojeny širokou škálou síťových technologií. Internet poskytuje širokou škálu informačních zdrojů a služeb, které jsou vzájemně propojeny, (World Wide Web (WWW), elektronická pošta, telefonie, sdílení souborů atd.).

Principy a předchůdci internetu byly používány v akademickém světě již zhruba od roku 1980, Využití internetu rychle od první poloviny devadesátých let rostlo. V Československu bylo první připojení k Internetu (první uzel) spuštěno v roce 1992.

Internet nemá svou centralizovanou správu ať již v technickém smyslu, nebo pro řízení politik týkajících se přístupu a používání; každá síť stanovuje své vlastní politiky. Pouze definice dvou hlavních jmenných prostorů v internetu, adresový prostor Internet Protocol (IP) a Domain Name System (DNS), jsou řízeny udržovací organizací Internet Corporation for Assigned Names and Numbers (ICANN). Nicméně existují komunitou odborníků vytvořená, široce akceptovaná a implementovaná technická doporučení, známá pod zkratkou RFC. Tato doporučení jsou schvalována a pravidelně aktualizována v rámci organizace Internet Engineering Task Force (IETF).

Pojem internet je tedy pojem používaný pro globální systém sítí propojených pomocí Internet Protocol. Obecně, ale ne zcela přesně, se pojem internet kolokviálně používá pro zkrácené označení sítě.

Pojmy internet a World Wide Web jsou často v každodenní řeči používány zaměnitelně (nepřesně); je běžné říkat "jdu na internet" při vyvolávání webového prohlížeče pro prohlížení webových stránek. Nicméně, World Wide Web neboli web je pouze jednou z velkého počtu internetových služeb.

3.2 Vysvětlení funkce poskytovatelů připojení k internetu

Obecně používaná charakteristika poskytovatele připojení k internetu je, že se jedná o osobu (komerční organizaci, komunitní složku, soukromou osobu, sdružení osob, neziskovou organizaci...) poskytující službu pro přístup další osoby k internetu. Poskytovatelé připojení k internetu využívají řadu technologií k tomuto připojení. Povaha a princip připojení pro účel tohoto odborného vyjádření hrají minimální či spíš žádnou roli.

4 Odpovědi na otázky

Otázka 1

Jaké osoby lze z Vašeho odborného pohledu ve vztahu k ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách v platném znění označit za poskytovatele připojení k internetu, respektive za poskytovatele připojení k internetu na území České republiky, jak tyto pojmy používá ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách, v platném znění?

Odpověď na otázku 1

Jeden z možných pohledů na definici poskytovatele internetového připojení (používána zkratka ISP z anglického Internet Service Provider, nebo IAP z Internet Access Provider) vychází ze zákona o elektronických komunikacích (ZEK)[2], který definuje podnikatele v oblasti elektronických komunikací. Jejich seznam je veden u ČTÚ.

Na tuto definici se však zákon č. 186/2016 Sb. neodkazuje. Podle tohoto výkladu je poskytovatelem každá firma, organizace, či jednotlivec, zprostředkující přístup k internetu další osobě. Může to tedy být jak ISP ve smyslu zákona o elektronických komunikacích, tak také například zaměstnavatel, umožňující svým zaměstnancům využívat připojení k Internetu. U mezinárodních společností pak může docházet k paradoxní situaci, kdy celá síť dceřiné společnosti využívá internetové připojení zahraniční matky, se kterou je propojena například přes pronajatý datový okruh a

[2] Zákon č. 127/2005 Sb., v platném znění.

využívá tak služeb zahraničního ISP. Také pokud společnost disponuje vlastním autonomním systémem, pak může být tento autonomní systém připojen pouze pomocí zahraničních poskytovatelů internetu. V obou těchto případech by povinnost blokovat internetové stránky dopadla na tyto mezinárodní společnosti, které by musely přístup k určeným stránkám blokovat a to navíc selektivně pouze pro zaměstnance z pobočky alokované v ČR. Do širší definice poskytovatele internetového připojení spadají také internetové kavárny, poskytovatelé bezplatné Wi-Fi konektivity (např. kluby, fast foody, letiště, čekárny, atd.) a dokonce i koncoví uživatelé, pokud své internetové připojení umožní využívat další osobě. Tento přístup je pak víceúrovňový, tzn., že další osoba v takovéto síti existující může snadno vytvořit vlastní bod přístupu (hotspot) a umožnit přístup dalším. Stává se tímto dalším poskytovatelem internetového připojení. Poskytovateli takovýchto služeb pak mohou být i zaměstnanci firmy, studenti škol, tedy návštěvníci všech prostor, kde jsou WI-FI dostupné. Speciální případ pak tvoří satelitní připojení. To znamená, že připojení k internetu není vázáno na území konkrétního státu (např. České republiky) a poskytovatel může sídlit v jiné zemi, než uživatel koncové služby.

Ve smyslu ustanovení § 82 odst. 1 zákona č. 186/2016 Sb. lze tedy za poskytovatele internetového připojení považovat každou osobu, která umožní připojení další osobě jak na komerční, tak i nekomerční bázi.

Otázka 2

Jak z Vašeho odborného pohledu chápete pojem internetová stránka ve vztahu k ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách v platném znění, jak tento používá ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách, v platném znění?

Odpověď na otázku 2

Výraz „internetová stránka" je nepřesný a nesprávně používaný. Znalec odkazuje na krátký terminologický slovník v tomto posudku a na kapitolu 3.1. **Správným výrazem z podstaty problematiky je „webová stránka".**

Ze Zákona není jasné, zdali se „internetovou stránkou" rozumí jen jedno URL nebo zdali se jedná o celou doménu (doménové jméno). Nastává zde pak vysoké riziko, že se zamezení dotkne dalších služeb (např. prohlížení informací) v doméně, které s předmětem zamezení přístupu k nepovoleným internetovým hrám nemají nic společného.

Otázka 3

Je technicky proveditelné zamezit v přístupu k internetovým stránkám, jak vyžaduje ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách, v platném znění a zároveň tak zajistit aby nebyly omezeny další poskytované a běžně využívané služby (e-mail, FTP atd.)?

Otázka 4

Jaká konkrétní technická opatření by bylo nezbytné přijmout v rámci plnění povinnosti zamezit v přístupu k internetovým stránkám ve smyslu ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách, v platném znění?

Otázka 5

Jaké by dle Vašeho odborného odhadu byly náklady na zavedení opatření pro zamezení v přístupu k internetovým stránkám, která jste vymezil v odpovědi na otázku č. 4?

Otázka 6

Bylo by možné zamezení v přístupu k internetovým stránkám ve smyslu ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách, v platném znění, provést technicky či ekonomicky efektivněji, než jak vyžaduje odkazované zákonné ustanovení?

Odpovědi na otázky 3, 4, 5 a 6

Analýza této problematiky

Odpovědi na tyto otázky jsou značně složité, protože existuje řada opatření a metod umožňující zamezení přístupu s různou účinností. Žádná z metod nezaručuje 100% účinnost a každá z metod má další efekty, které je nutné zohledňovat. Zároveň pak každá metoda sebou nese různě vysoké finanční i časové náklady na realizaci. Proto se znalec rozhodl tyto 4 otázky diskutovat společně a odpovědi na ně vyjádřit v tabulce, která vazby ilustruje. Zohledněné aspekty včetně nákladů nelze vyjádřit přesněji, nežli ve třech stupních – nízká, střední, vysoká (popř. extrémně vysoká).

Tabulka 1 ilustruje současné technické a technicky použitelné metody blokování přípustné v duchu ustanovení §82 odst. 1 zákona č. 186/2016 Sb. Tabulka byla vytvořena tak, že pro jednotlivé, znalcem identifikované metody, byly určeny aspekty zamezení z hlediska jejich:

a. Účinnosti;
b. Negativního dopadu;
c. Nákladů na realizaci;
d. Možnosti obejití opatření.

Vysvětlení použitých aspektů zamezení:

- Účinnost – zdali lze stránku z území České republiky blokovat a to pro všechny uživatele, zdali tomu může provozovatel bránit a najít jiné řešení.
- Dopad v negativním smyslu – zamezení dalších služeb, které nejsou v rozporu se Zákonem a dalším stránkám s podobnými následky.
- Náklady – náklady na realizaci nutných opatření pro zamezení blokace.
- Možnost obejití opatření uživatelem použitím alternativních způsobů připojování do sítě internet. Například pomocí komunikace Klient-server, mobilní aplikace, atp.

Metoda	Účinnost	Negativní dopad	Náklady	Možnost obejití opatření	Poznámka
Blokování na bázi HTTP	malá - nepostihuje HTTPS	nízký	vysoké	vysoká	Blokování na úrovni HTTP je možné použitím HTTPS a tím tuto metodu blokování velmi snadno obejít.
Blokování na úrovni lokálního DNS serveru	vysoká z pohledu provozovatele	vysoký	nízké	extrémně vysoká	Blokuje další služby jako např. E-mail i další stránky pod tímto DNS
Blokování IP adresy	nízká	vysoký	nízké	vysoká	Blokuje další služby jako např. E-mail i další stránky i celý sdílený hosting a další subjekty.

Metoda	Účinnost	Negativní dopad	Náklady	Možnost obejití opatření	Poznámka
Vynucené použití proxy serveru na úrovni poskytovatele internetových služeb	vysoká	nízký	extrémně vysoké	vysoká	Používá se běžně na úrovni organizací. Na úrovni poskytovatele připojení by tato metoda byla extrémně náročná a špatně kontrolovatelná.

Vysvětlení jednotlivých metod blokování:

U každé metody uvádí znalec přesnější popis blokování a také krátký rámcový popis možného obejití tohoto blokování.

Blokování na bázi HTTP

Blokování

Blokování na bázi HTTP je možné provádět filtrováním veškerého HTTP provozu. Podmínkou filtrování je přesměrování HTTP provozu ze sítě ISP na jeden, nebo více serverů, které budou toto filtrování provádět. Na těchto serverech pak specializovaná aplikace nahlíží do hlaviček protokolu HTTP a na základě jejich vyhodnocení může zablokovat konkrétní URL. Cena takovéhoto řešení se odvíjí od množství klientů v síti a tím také výpočetního výkonu potřebného pro realizaci filtrace.

Obejití

Ač je tato metoda velmi přesná, pokud jde o zacílení blokované služby až na úroveň konkrétní URL, není bohužel účinná při použití HTTPS, tedy šifrované komunikace. V případě šifrovaného přenosu totiž není možné sledovat obsah hlavičky protokolu HTTP, neboť ten je také šifrovaný. Zároveň je třeba zdůraznit, že připojení využívající HTTPS je dnes běžnou součástí webových stránek umožňující finanční transakce. Metodě blokování se lze vyhnout i použitím VPN, webových prohlížečů Tor a dalších podobných služeb, postavených na šifrovaném přenosu paketů.

Blokování na úrovni lokálního DNS serveru

Blokování

Blokování na úrovni lokálního DNS serveru znamená, že tento DNS server nebude klientům vracet odpovědi pro definovaná doménová jména. Při standardní DNS komunikaci klient odesílá DNS serveru dotaz, kde se ptá, jakou IP adresu má daná konkrétní doména, například www.mfcr.cz. Server pak zajistí a vrátí odpověď klientovi a ten pak může zahájit komunikaci s konkrétním uzlem sítě. Na jedné IP adrese však může běžet a v praxi tomu tak také často bývá, veliké množství dalších služeb. Zablokování na úrovni lokálního DNS serveru má tedy přímý dopad na všechna URL na dané doméně, nejen na jedno konkrétní, ale navíc může postihnout i uživatele jiných služeb, které se na dané doméně nacházejí (např. E-mail).

Obejití

Nastavit si jiný volně dostupný DNS server (např. DNS servery společnosti Google) není obtížné ani pro běžného uživatele bez odborných znalostí, který tak může snadno obejít blokaci prováděnou jeho lokálním ISP. I pokud by ISP prováděl blokaci odchozí DNS komunikace, tak aby jeho klienti byli nuceni používat pouze jeho lokální DNS, stále existují další jednoduché možnosti, jak toto blokování obejít. Jednou z nich je zadání blokované informace do lokálního souboru hosts, který existuje na všech platformách a jehož obsah má přednost před informacemi z DNS serveru. Jinými slovy, pokud je v souboru hosts definováno, že doménové jméno www.mfcr.cz má IP adresu XXX.XXX.XXX.XXX, nebude žádný DNS dotaz proveden a bude rovnou zahájena komunikace s daným serverem.

Blokování IP adresy

Blokování

Blokování konkrétní IP adresy se obvykle realizuje na síťových zařízeních pomocí tzv. Access control list (ACL). V takovém případě jsou monitorovány hlavičky protokolu IP a je sledována cílová IP adresa paketu. Pokud je nalezena IP adresa z ACL, pak je paket zahozen. Vzhledem k nedostatku IPv4 adres (dosud používaný systém adresace), i k ekonomickým úsporám je běžným standardem kumulovat na jedné IP adrese velké množství služeb. Nejen, že webhostingové společnosti mohou tedy v rámci sdíleného webhostingu provozovat tisíce webových stránek na jedné jediné IP adrese, ale je i běžné na jedné IP adrese provozovat více různých internetových služeb. Blokování IP adres by tedy vedlo k totálnímu zablokování všech webových stránek a dalších internetových služeb na dané IP adrese.

Obejití

Toto filtrování lze navíc snadno obejít, pokud pro přenos paketu využiji nějakou z forem tunelování. Zjednodušeně lze říci, že cílová IP adresa paketu směřuje na IP adresu neuvedenou v ACL a teprve na zařízení na této IP adrese dojde k rozbalení původní informace a jejímu doručení na zařízení s IP adresou, která má být blokována. Stejnou cestou pak data proudí zpět k uživateli, tedy opět přes IP adresu, která není v ACL blokována. Toto přeposílání lze v závislosti na použité technologii řetězit mezi více uzlů, obsah přenášených dat je také obvykle šifrován, přenos informace k zakázanému uzlu tak nelze detekovat ani při použití hlubší analýzy paketů.

Vynucené použití proxy serveru na úrovni poskytovatele internetových služeb

Blokování

Filtrování na bázi proxy serveru je celkem běžně používané na úrovni organizací, kde je možné vzhledem k množství zařízení jednoduše zajistit nastavení koncových stanic. Proxy server funguje jako prostředník mezi klientem a serverem, kdy z pohledu serveru je komunikující stranou (klientem) proxy server. Samotné filtrování pak probíhá na proxy serveru, kde může správce jednoduše nastavit, která URL mají být uživatelům dostupná. To činí tuto metodu podobně přesnou, jako blokování na bázi HTTP. Informace o použití proxy však musí být na koncové stanici nastavena administrátorem. Pokud by tedy ISP k této technologii přistoupil, znamenalo by to ruční rekonfiguraci stovek tisíc koncových stanic zákazníků a tedy obrovské náklady pro poskytovatele internetu.

Obejití

I v tomto případě však může uživatel využít možností, popsaných v předchozí části a blokování obejít např. pomocí tunelování paketů.

Shrnutí popsaných metod blokování

Jak snadno se dá příslušná metoda blokování obejít, není možné obecně stanovit a to ani technicky ani finančně. Každý poskytovatel připojení k internetu může mít zcela odlišnou architekturu svých technologií a to od platformy až po portfolio svých služeb.

Možnost, jak snadno půjde konkrétní blokovací technologie obejít, je často velice úzce závislá na finanční náročnosti daného řešení. Obecně lze konstatovat, že čím je daná technologie blokování levnější, tím snadněji jde obejít. Jako příklad lze uvést blokování na úrovni lokálního DNS serveru, které je sice pro poskytovatele připojení k internetu finančně relativně nenáročné, avšak pro koncového uživatele snadno obejitelné.

Odpověď na otázky 3, 4, 5 a 6

Zamezení přístupu není nikdy 100% možné[3] . Není možné zajistit, aby byl zároveň zamezen přístup k internetovým stránkám, jak vyžaduje ustanovení § 82 odst. 1 zákona č. 186/2016 Sb., o hazardních hrách, v platném znění a zároveň zajistit, aby nebyly omezeny další poskytované a běžně využívané služby. Každá metoda zamezení přístupu sebou nese i další rizika (technická i jiná), která mohou buď značně zvýšit náklady na realizační opatření, a to nad hranici únosnosti a zároveň mohou přinést i možná vyhnutí se zamezení přístupu. Tím se účinnost celého tohoto opatření snižuje. Běžně používaný způsob připojení do vzdálené sítě (např. firmy, partnera apod.) se provádí pomocí jistých „tunelů" (typu VPN), který vždy umožní obejití technických i dalších kontrol poskytovatele připojení k internetu a i dalších na trase od uživatele k cílové webové stránce. Není možné zamezit použití[4] těchto tunelovacích technik na úrovni poskytovatele připojení k internetu. Tyto techniky v drtivé většině případů používají navíc šifrování, takže jakákoliv inspekce je legálně vyloučená.

Otázka 7

Existuje možnost hraní internetové hazardní hry bez použití internetových stránek?

Odpověď na otázku 7

Ano.

Existují například aplikace pro mobilní i desktopové operační systémy (využívaných dnes na chytrých telefonech, tabletech i osobních počítačích, atd.), které nepoužívají webové (internetové stránky), ale přistupují přímo k datovým zdrojům. Tyto aplikace se pro internetové hazardní hry již používají a jejich obliba rychle roste, stejně jako obecně roste obliba používání mobilních aplikací. Poskytují totiž uživatelům daleko lepší komfort při hraní, jsou pro uživatele intuitivnější. A protože se v nich lépe hraje, jsou uživatelsky atraktivnější. Provozovatelům internetových hazardních her se tedy vyplatí takové aplikace svým uživatelům poskytovat.

Tyto aplikace se pro internetové hazardní hry (on line sázení) již používají a jsou dostupné většinou zdarma. Zájemce o tento typ hraní internetových hazardních her si pak pouze stáhne aplikaci do svého chytrého telefonu a poté již k žádným webovým stránkám přistupovat nemusí.

Znalec zde odkazuje na dvě z mnoha běžně dostupných nabídek těchto aplikací pro chytré telefony:

- http://verifikace.com/sazeni - Mobilní sázení: Sázení přes mobil je možné buď prostřednictvím mobilní verze stránky, nebo mobilní aplikace příslušné sázkové kanceláře. Mobilní sázkové aplikace se vytvářejí především pro operační systémy Android, iOS (iPhone, iPad), Windows Phone a BlackBerry. Výhodami mobilního sázení jsou rychlost, jednoduchost a možnost uzavřít sázku kdekoliv a kdykoliv.
- http://www.ifortuna.cz/cz/sazeni/mobilni_sazeni/.

Tím znalec zodpověděl všechny otázky a splnil úkol zadavatele.

---

[3] Viz definice webové stránky

[4] Toto zamezení by přineslo brutální zásah do široké škály legitimního používání těchto prostředků.

5 ZÁVĚR - ZNALECKÁ DOLOŽKA

Znalecký posudek jsem podal jako znalec jmenovaný rozhodnutím ministra spravedlnosti ČSR dekretem čj. ZT 1817/82, ze dne 4. 8. 1982 a 18. 10. 1984, pro obor kybernetika, odvětví výpočetní technika specializace elektronické součásti a obor ekonomika, odvětví ceny a odhady se specializací elektronika a výpočetní technika s rozšířením na odhady cen pro zahraniční elektroniku ze dne 26. 11. 1987.

Znalec ve smyslu § 127 a zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů, prohlašuje, že si je plně vědom následků vědomě nepravdivého znaleckého posudku.

Tento posudek je zapsán ve znaleckém deníku pod pořadovým číslem 1483/2016. Posudek obsahuje 12 (dvanáct) listů a je vyhotoven šestkrát (pět kopií pro žadatele a jedna pro archiv znalce).

V Praze dne 29. 08. 2016

Ing. Jan Fanta, CISA, CRISC
Kolínská 14
130 00 Praha 3