20. 4. 2020

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Trestní postih DoS/DDoS útoků

V právní teorii i praxi vyvstává otázka, zda kybernetické útoky typu DoS či DDoS je možné považovat jako trestný čin. Ačkoliv je DoS/DDoS útok obecně považován za formu kyberkriminality, je vůbec možné takový typ útoků postihovat dle českého trestního zákoníku?

Dle policejních statistik je zcela evidentní nárůst počítačové kriminality[1], kdy typickým útokem řazeným mezi formu počítačové kriminality je právě útok typu DoS/DDoS.

DoS (Denial of Service) představuje kybernetický útok typu odepření služby, při kterém dojde k zahlcení cílového serveru vysláním obrovského množství požadavků. Cílový server pak není schopen takové množství dat zpracovat a dochází k jeho přetížení, nefunkčnosti a nedostupnosti služby u ostatních oprávněných uživatelů. Při tomto typu útoku však fakticky nedochází k průniku útočníka do cílového systému, resp. útočník nezískává možnost data získat či s daty. Rozšířenou variantou útoku je pak DDoS (Distributed Denial of Service), kdy k útoku nedochází z jednoto počítače, ale z většího množství počítačových systémů. DoS a DDoS (souhrnně označeny jako (D)DoS) tak představují dva základní typy kybernetických útoků, které jsou zaměřeny na znepřístupnění služby.

Trestněprávní kvalifikace útoku typu (D)DoS není bohužel z pohledu českého trestního zákoníku zcela jednoznačná, což ostatně dokazuje také postup orgánů činných v trestním řízení, které mají tendenci věc odkládat s tím, že se nejedná o trestný čin. Tato nejednoznačnost vyplývá z poměrně nešťastně formulovaných skutkových podstat trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací ve smyslu ust. § 230 odst. 1 a 2 trestního zákoníku.

Česká republika je od roku 2013 vázána Úmluvou o počítačové kriminalitě (dále jen „Úmluva“)[2]. Dle této Úmluvy musí smluvní státy přijmout taková legislativní a jiná opatření, která budou nezbytná k tomu, aby podle jejích vnitrostátních právních předpisů bylo trestným činem, pokud je spácháno úmyslně, neoprávněné poškození, vymazání, snížení kvality, pozměnění nebo potlačení počítačových dat.[3] Právě pod pojem „potlačení počítačových dat“ je třeba podřadit (D)DoS útoky. Strany Úmluvy jsou dále povinny přijmout taková legislativní a jiná opatření, která budou nezbytná k tomu, aby trestné činy ve smyslu Úmluvy bylo možno potrestat účinnými, přiměřenými a odrazujícími tresty, včetně trestu odnětí svobody.[4] Je tedy evidentní, že ve smyslu Úmluvy, kterou je Česká republika vázána, jsou (D)DoS útoky považovány za trestné činy.

Trestní postih (D)DoS útoků pak vyžaduje také směrnice Evropského parlamentu a Rady č. 2013/40/EU ze dne 12.3.2013. Dle této směrnice členské státy přijmou nezbytná opatření k zajištění toho, aby úmyslné a neoprávněné závažné narušení nebo přerušení fungování informačního systému vložením počítačových údajů či jejich přenosem, poškozením, vymazáním, znehodnocením, pozměněním, potlačením nebo znepřístupněním bylo trestným činem, a to alespoň tehdy, pokud se nejedná o méně závažný případ.[5] (D)DoS útok pak ve smyslu této směrnice představuje přerušení fungování informačního systému potlačením nebo znepřístupněním.

Je však předmětem polemiky, zda i současné znění trestního zákoníku umožňuje postihovat páchání těchto útoků tak, jak vyžadují shora zmíněné mezinárodní závazky. Útočník při (D)DoS útoku může naplnit skutkovou podstatu trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací dle ust. § 230 odst. 2 písm. b) trestního zákoníku, podle kterého se trestného činu dopustí ten, kdo získá přístup k počítačovému systému nebo k nosiči informací a data uložená v počítačovém

systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými. Uvedená skutková podstata vyžaduje, aby útočník získal přístup k počítačovému systému, což však neodpovídá požadavkům Úmluvy a směrnice, které za trestné považují úmyslné jednání spočívající v potlačení či znepřístupnění počítačových dat bez požadavku získání přístupu k systému. Při (D)DoS útocích útočník přístup k systému nezískává v tom smyslu, že by data v sytému mohl získat, pozměnit či jinak s nimi nakládat. Na první pohled by se tedy mohlo dojít k závěru, že tyto útoky dle citovaného ustanovení postihnout nelze právě z důvodu absence přístupu k počítačovému systému.

(D)DoS útoky za trestný čin dle trestního zákoníku nepovažuje ani část právní vědy. Například Jan Kolouch uvádí, že „zřejmě díky neznalosti technické stránky věci či díky potřebě právního popsání jednání, které má povahu DoS či DDoS útoků, došlo ke vzniku právní normy, která v praxi postih za provedení útoku DoS či DDoS neumožňuje.[6] Uvedený názor je také přebírán policejními orgány při vyšetřování trestných činů, kdy ze strany policie nejsou (D)DoS útok považovány za trestný čin. Dokonce se lze setkat s odůvodněním policejního orgánu, že (D)DoS útok nejen není trestným činem, ba dokonce nejde ani o jednání protiprávní. Takovéto právní posouzení, které vylučuje posouzení (D)DoS útoků jako trestný čin, považuji za zcela nesprávné. Ostatně za DDoS útoky či pokus o DDoS útok již byly českými soudy útočníci pravomocně odsouzeni.

Tak například došlo k odsouzení pachatele za DDoS útok na internetové stránky Úřadu vlády[7] či za pokus DDoS útoku na internetové stránky České strany sociálně demokratické[8]. Ve druhém případě rozhodoval také Nejvyšší soud, který uzavřel, že skutková zjištění popisující pokus o provedení DDoS útoku výstižně obsahují všechny znaky trestného činu neoprávněného přístupu k počítačovému systému a nosiči informací.[9] Soudy v tomto případě považovaly za naplnění znaku přístupu k počítačovému systému to, že by útočník překonal bezpečností opatření, a právě tím získal přístup k počítačovému systému. Jinak řečeno, pokud by útočník neprovedl DDoS útok, nepřekonal by bezpečnostní opatření serveru, pak by vůbec neměl přístup k počítačovému systému nad rámec standardního užití ze strany běžných uživatelů. Tento závěr je dle mého názoru správný a odpovídá také mezinárodním závazkům k trestání (D)DoS útoků.

Pro doplnění lze uvést, že při provedení (D)DoS útoku bude téměř vždy naplněna zvláště přitěžující okolnost podmiňující použití vyšší trestní sazby dle ust. § 230 odst. 3 písm. a) či b) trestního zákoníku, neboť úmyslem útočníka v tomto případě je omezení funkčnosti systému, popř. způsobení škody provozovateli.

Lze uzavřít, že i přesto, že z čistě jazykového výkladu příslušných ustanovení trestního zákoníku neplyne, že by útoky typu (D)DoS trestní zákoník postihoval, neboť vyžaduje získání přístupu k počítačovému systému, který v užším slova smyslu pachatel nezískává, je třeba tyto útoky postihovat dle ust. § 230 odst. 2 písm. b) trestního zákoníku. Za neoprávněný přístup je třeba považovat právě překonání bezpečnostních opatření, které by měly (D)DoS útokům bránit. De lege ferenda lze však jednoznačně doporučit úpravu či rozšíření skutkových podstat tak, aby postih (D)DoS útoků jednoznačně odpovídal mezinárodním závazkům a také faktickému způsobu provedení (D)DoS útoků.

Mgr. Bc. Jakub Šťastný,
advokát

Tel.: +420 731 906 390
E-mail: jakub@stastny-advokat.cz

[1] Kyberkriminalita [online]. [cit. 19.3.2020]. Dostupné na https://www.policie.cz/clanek/kyberkriminalita.aspx

[2] Sdělení Ministerstva zahraničních věcí o sjednání Úmluvy o počítačové kriminalitě ze dne 23.12.2013

[3] Čl.4 odst. 1 Úmluvy

[4] Čl. 13 odst. 1 Úmluvy

[5] Čl. 4 směrnice

[6] KOLOUCH, Jan, CyberCrime. 1. vydání. Praha: CZ.NIC, z. s. p. o., 2016, str. 301

[7] Trestní příkaz Okresního soudu v Ostravě ze dne 13.8.2018, sp. zn. 11 T 85/2018

[8] Rozsudek Okresního soudu v Rychnově ze dne 30.4.2018, sp. zn. 2 Tm 11/2017

[9] Usnesení Nejvyššího soudu ze dne 13.2.2019, sp. zn. 8 Tdo 100/2019

Další články:

- Trestní odpovědnost provozovatelů anonymních sítí
- Oprávnění policejního orgánu k odemknutí mobilního telefonu nuceným přiložením prstu obviněného
- Adhezní řízení v praxi
- Novela trestního zákoníku
- Otevřel Ústavní soud zákonodárci dveře k uzákonění eutanazie v České republice?
- Velká reforma trestního práva, jak moc velká je?
- K odpovědnosti státu za majetkovou a nemajetkovou újmu způsobenou při výkonu veřejné moci. Vyslovování konstatací porušení práva. Připomínka státního svátku 6. července
- Právní novinky v roce 2025, část čtvrtá – implementace nové definice domácího násilí
- Právní novinky v roce 2025, část třetí – změny v oblasti veřejných zakázek a v trestním právu
- K aplikaci zásady in dubio pro reo v rámci řízení o povolení obnovy trestního řízení
- Trestný čin poškození věřitele