**V Austrálii došlo ke kybernetickému útoku na parlament, odborníci podezřívají Čínu**

**Praha, 12. února 2019 – *Sofistikovaný kybernetický útok s cílem získat přístup k citlivým datům a politicko-strategickým informacím australského parlamentu se odehrál v pátek 8. února před očekávanými parlamentními volbami. Odborníci na kybernetickou bezpečnost se shodují, že podle způsobu provedení útoku, který byl zaměřen na získání důvěrné neveřejné komunikace mezi předsedou vlády a ostatními politickými lídry, mohl být organizován a financován čínským režimem.***

„*To, co se odehrálo v pátek, naznačuje snahu o ovlivnění nadcházejících voleb a zdiskreditování určitých politiků či politické strany*,“ komentuje útok Martin Půlpán, generální ředitel společnosti net.pointers. Čína je pro Austrálii největším obchodním partnerem a díky strategickým surovinám a vyspělé ekonomice Austrálie se v této zemi snaží upevnit svůj politicko-ekonomický vliv a hájit tak své zájmy, které jsou však často v rozporu se současnou politikou Austrálie.

Útok se v současné chvíli intenzivně vyšetřuje, avšak získat přímé důkazy o propojení s Čínou je z povahy internetu a sofistikovanosti útoku velmi obtížné. „*Odborníci na kybernetickou bezpečnost se však shodují, že podle způsobu útoku, použitých nástrojů a dalších indicií může jít o útok organizovaný a financovaný čínským režimem*,“ říká Půlpán a dodává: „*Obezřetnost vůči aktivitám Číny v oblasti kybernetických útoků, špionáže a ovlivňování veřejného mínění je tak určitě namístě a potvrzují to i další nedávné útoky na australské státní organizace spojované s aktivitami řízenými z Pekingu. Konkrétním příkladem je útok na Bureau of Meteorology z roku 2015, který je úzce napojen na výzkum a vývoj v australském obranném průmyslu, či pokus o zcizení strategických plánů a zabezpečení komunikační infrastruktury nových vládních budov v Canbeře z roku 2013.*“ V loňském roce pak proběhl další velký kybernetický útok, a to na pět velkých australských webhostingových providerů, který je s Čínou rovněž spojován.

Obezřetnost vůči čínskému režimu v oblasti kybernetické bezpečnosti je kvůli speciální armádní jednotce PLA UNIT 61398, kterou disponuje čínská vláda, opodstatněná. Jednotka se specializuje na kybernetické útoky, hacking a je spojována například s intenzivními kybernetickými útoky na americké společnosti v roce 2013.

**O net.pointers**Ryze česká společnost net.pointers, s.r.o., se zaměřuje na kybernetickou bezpečnost a oblast unified communications. Působí ve střední Evropě, na Blízkém východě a v asijsko-pacifickém regionu. Firma disponuje zkušenostmi v oblastech prevence a ochrany komunikačních sítí proti kybernetické kriminalitě, ochrany proti útokům DDoS, forenzních analýz, unified communications a vzdělávání v kybernetické bezpečnosti. Poskytované služby zahrnují profesionální zákaznickou podporu, zavádění technologií, managed security services a kontinuální vývoj softwaru, včetně vývoje vlastních aplikací a SW nadstaveb.

**Kontakt pro média
Stance Communications, s.r.o.**
Tereza Schneiderová
Account Manager
Jungmannova 750/34, 110 00 Praha 1
Tel.: +420 724 872 331, +420 224 810 809
E-mail: tereza.schneiderova@stance.cz