Stanovisko Pirátů ke kybernetické bezpečnosti

Pirátská strana je silným zastáncem digitálně propojené společnosti, digitalizovaného a efektivního státu, transparentnosti veřejné správy a ochrany soukromí a osobních dat občanů. Právě proto si Piráti uvědomují hrozby i výzvy dnešního digitálního světa a považují kybernetickou bezpečnost za zásadní prvek kvalitního výkonu státní správy a prosazování bezpečnostních zájmů ČR. Pirátská strana má vizi, jak zajistit, že bude naše společnost zabezpečena vůči výzvám budoucnosti.

Kybernetická bezpečnost státu

Mezinárodní právo

Na působení států v kyberprostoru[1] se vztahuje mezinárodní právo. To zahrnuje zejména Chartu Organizace spojených národů, Evropskou úmluvu o ochraně lidských práv a svobod a závazky v Severoatlantické alianci. Česká republika by i pro doménu kyberprostoru měla uznávat závazky každého státu vyplývající z principu suverenity: zdržet se hrozby silou nebo použití síly; řešit spory mírovou cestou; a zdržet se zasahování do vnitřních záležitostí jiných států.

Piráti podporují důsledné dodržování Norem OSN odpovědného chování státu v kyberprostoru[2], tedy jedenácti dobrovolných a nezávazných pravidel, která vytváří základ pro kolektivní očekávání ohledně chování států v kyberprostoru.

Piráti podporují Rozhodnutí Stálé rady OBSE o opatřeních pro budování důvěry, ke snížení rizika konfliktu na základě používání informačních a komunikačních technologií[3] a podporují aktivní zapojení ČR do implementace těchto opatření ve spolupráci se Sekretariátem OBSE.

Piráti se zasazují o tvorbu jasné pozice České republiky k jednotlivým principům mezinárodního práva tak, aby bylo zřejmé, jaký mezinárodněprávní výklad ve vztahu ke kybernetickému prostoru zastáváme. Došlo by tím mimo jiné i ke zvýšení transparentnosti při jednání se spojenci a podobně smýšlejícími státy.

---

[1] Kyberprostor je globální a vyvíjející se doména popisovaná užíváním elektrických sítí a elektromagnetického spektra, jejíž smysl je vytvářet, uchovávat, upravovat, vyměňovat, sdílet, vybírat, používat či vymazávat informace. Kyberprostor zahrnuje: a) fyzická i telekomunikační zařízení, která umožňují spojení technologií a komunikaci sítí systému, chápáno obecně (SCADA zařízení, smartphony/tablety, počítače, servery, atd.), b) počítačové systémy a komplementární software, který zaručuje spojení a funkčnost systému, c) spojení počítačových sítí, d) uživatelské vstupy a uzly zprostředkovatelů spojení, e) informace – uživatelská data. https://cs.wikipedia.org/wiki/Kyberprostor#cite_note-6

[2] Normy OSN odpovědného chování státu v kyberprostoru: https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf

[3] Rozhodnutí Stálé rady OBSE: https://www.osce.org/files/f/documents/d/a/227281.pdf

Odpovědnost za útok

Součástí ochrany demokracie je poskytování informací občanům tak, aby se dokázali účinně bránit manipulacím, dezinformacím či propagandě. Občan musí být schopen informovaného rozhodnutí. Piráti proto prosazují zkvalitnění komunikace státu směrem k veřejnosti i v oblasti kybernetických útoků.

Dojde-li ke kybernetickému útoku, je nutné vzít v potaz negativní vliv informačního vakua na veřejnost a poskytnout zavčas občanům informace o útoku. Případně, je-li možné s vysokou mírou jistoty provést atribuci, tak i o tom, kdo za útokem stojí[4]. Pokud je míra jistoty nízká či existují pádné důvody pro ochranu takové informace, například kvůli ochraně zdroje, je nezbytné komunikovat důvody.

Veřejnou atribuci by měla doporučit vládě Bezpečnostní rada státu na základě informací pracovní skupiny skládající se z expertů Národního úřadu pro kybernetickou a informační bezpečnosti, všech tajných služeb, Nejvyššího státního zastupitelství, Policie ČR a dotčených ministerstev. Informace pracovní skupiny by měly být dostupné v rozsahu nezbytném k přezkoumání doporučení.

Piráti také prosazují jasně nastavený státní systém reakce založený na škálování a jasných kvalitativních i kvantitativních parametrech. Tedy jak z hlediska množství útoků za určitou dobu, tak dopadů na suverenitu, bezpečnost, majetek i zdraví občanů. Systém by měl umožňovat i určit pravděpodobnost, s jakou je určitý aktér za kybernetický útok zodpovědný. Útočníci musí vědět, že kyberprostor není beztrestná zóna a že Česká republika je připravena v úzké koordinaci se spojenci své oprávněné zájmy v kyberprostoru legálními metodami bránit. To může zahrnovat i aktivní působení za účelem minimalizace následků probíhajícího útoku či preemptivní operace.

Ochrana kritické infrastruktury

Bezpečnost systémů kritických pro chod státu i společnosti je ohrožena kybernetickými útoky stejně jako prostřednictvím nedůvěryhodných dodavatelů a dodavatelských řetězců, které se stávají prostředkem k prosazování politických cílů a geopolitických zájmů.

Subjekty kritické infrastruktury

Subjekty kritické infrastruktury dle aktualizované Směrnice EU o Informačních sítích (NIS 2[5]), kterou je stanovena minimální úroveň kybernetického zabezpečení proti útokům, jsou:

- Zásadní subjekty podléhající nejvyššímu stupni ochrany: energetický sektor; doprava; bankovnictví; infrastruktura finančních trhů; poskytovatelé zdravotní péče, výrobci léčiv a zdravotnických prostředků; správa vodních a odpadních sítí; digitální infrastruktura; veřejná správa; vesmírný výzkum.

[4] Atribuce je přičtení odpovědnosti za kybernetický útok konkrétnímu aktérovi na základě forenzních šetření nebo jinak získaných informací a stop.
[5] NIS 2 informační stránka NÚKIB: nis2.nukib.cz

- Významné subjekty povinně dodržující ochranná opatření a pravidla: poštovní a kurýrní služby; nakládání s odpady; výroba, zpracování a distribuce chemikálií; výroba, zpracování a distribuce potravin; zpracovatelský průmysl; digitální poskytovatelé.

Mezi významné subjekty by se podle Pirátů měla zařadit také špičková vědecká a výzkumná pracoviště, která čelí zvyšujícímu se počtu kyberútoků a zahraničním vlivovým operacím, stejně jako krádežím citlivých dat a know-how ze strany nedemokratických režimů.

Piráti také budou usilovat o vylepšení koordinace expertů na kyberbezpečnost prostřednictvím společné platformy a sdílení informací nezbytných pro lepší ochranu. To podle nás povede k prohloubení povědomí a zefektivnění procesů pro předcházení a zvládání kybernetických incidentů, a také zefektivnění reakcí na útoky.

Dodavatelský řetězec

Hardware i software technologických řešení v rámci naší kritické infrastruktury je již natolik komplexní, že snižovat rizika spojená s dodavateli pouze technickými prostředky je nedostatečné. Zásadním faktorem je tudíž důvěryhodnost dodavatele, a to již na strategické úrovni v souvislosti s právním a politickým prostředím, ze kterého dodavatel operuje.

Česká republika reagovala jako jedna z prvních zemí na hrozbu kompromitace 5G sítí ze strany nedůvěryhodných dodavatelů (např. společností Huawei) formulací a přijetím nezávazných doporučení, které je ale potřeba adekvátně rozšířit na celou kritickou infrastrukturu.

Piráti chtějí jasná a transparentní kritéria pro hodnocení nabídek v rámci veřejných zakázek pro kritickou infrastrukturu, která budou reflektovat i důvěryhodnost dodavatelů z pohledu kyberbezpečnosti. Mezi tato kritéria by mělo patřit dodržování mezinárodního práva, lidských práv a právního státu v zemi, do jejíž jurisdikce dodavatel spadá, a to včetně jeho subdodavatelů. Dodavatel by měl být ochoten zavázat se prohlášením, že neposkytne důvěrné informace o svých zákaznících třetím stranám (včetně mateřských, sesterských společností apod.) s výjimkou legálního soudního příkazu, a rovněž transparentně prokázat svou vlastnickou strukturu.

Piráti také podporují východiska uvedená v Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v ČR[6], podle nichž lze hodnotit důvěryhodnost dodavatelů i v případě dalších systémů kritické infrastruktury.

Strategická autonomie

Piráti podporují koncept strategické autonomie na evropské úrovni, tedy budování vlastních kapacit a posilování nezávislosti na rozhodnutí jiných. V tomto směru by ČR ve spolupráci s dalšími členy EU a spojenci z NATO měla usilovat i o surovinovou bezpečnost, resp. o zajištění dostatku surovin kritických pro výzkum a vývoj nových technologií. Je nežádoucí, aby náhlý výpadek kritických surovin či technologií způsobil významné narušení bezpečnosti a společenské solidarity.

[6] Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice: https://www.nukib.cz/download/aktuality/5G-Doporuceni_CZ.pdf

Piráti proto podporují aktivní budování strategicky výhodných průmyslových kapacit, stejně jako podporu talentů, vědeckých týmů a know-how na národní i evropské úrovni a jejich udržování v rámci Evropy skrze motivační pobídky. V souladu s konceptem strategické autonomie by také Česká republika a EU měly systematicky a intenzivně podporovat vědecký sektor, chránit vědecká pracoviště před cizím vměšováním a únikem citlivých dat a poskytovat jim bezpečnou infrastrukturu pro ochranu výsledků výzkumu a vývoje před útočníky.

S tím souvisí také digitální suverenita, tedy zabezpečení vždy dostupného a dle aktuálních potřeb upravitelného software pro provozování kritické infrastruktury i zajišťování důležitých funkcí státu. Piráti proto podporují maximální využívání evropských řešení a svobodného software v systémech veřejné správy. Piráti dále podporují vytvoření specializované státní agentury nebo pověření existujícího orgánu vývojem unifikovaných softwarových řešení založených na svobodném software a použitelných napříč různými úrovněmi státní správy, počínaje vytvořením standardního pracovního prostředí.

Občanské zapojení

Důležitou součástí kyberobrany státu by měli být jeho občané, a to jak ti aktivně zapojení, tak pasivně poučení a informovaní. Piráti podporují důraz na vzdělávání společnosti v oblasti kyberbezpečnosti a ochrany soukromí, které musí začínat již u studentů základních a středních škol. Zásadní je také podpora vysokoškolských aktivit (např. budování společných interdisciplinárních pracovišť a platforem nebo otevírání nových vysokoškolských oborů) a adekvátní finanční ohodnocení kyberexpertů ve státní správě. Nejsou-li podmínky zaměstnání kompetitivní, stát se vystavuje závislosti na soukromých dodavatelích.

Stát by měl také podporovat angažovanou občanskou společnost a dávat prostor organizacím sdružujícím nezávislé odborníky, aby se mohli podílet na zajišťování kybernetické obrany státu a bezpečnosti státních institucí. Nástrojem takové podpory mohou být hackatony či poskytování kontrolovaného prostředí pro penetrační testování systémů státních institucí a kritické infrastruktury.