Bezpečnost v kybernetickém světě, nad kterou se musí přemýšlet

10.9.2024 - | PROTEXT

Nejvýznamnějším dokumentem, který bude v následujících letech vymezovat mantinely používání umělé inteligence v Evropě, je Akt o AI, který byl unijními ministry schválen v květnu letošního roku. Ten je podle místopředsedy vlády Ivana Bartoše, pro digitalizaci dobře uchopen: „V Aktu o umělé inteligenci jsme se snažili vyvážit několik principů. Nenasměrovat to do té dystopické budoucnosti, války strojů a umělých inteligencí, ale k tomu, abychom AI dokázali ochočit, rozvíjet a využít.“ Na implementaci mají členské státy dva roky a způsob, jakým se jí zhostíme, je podle Bartoše velmi důležitý. „Byl bych nerad, kdyby to dopadlo tak, že Amerika má AI, Čína má AI a my máme dobrou regulaci.“

Před přílišnou regulací varoval na diskuzi Zlaté koruny i ředitel Národního úřadu pro kybernetickou bezpečnost Lukáš Kintr. *„Kyberbezpečnost je jen jeden dílek, s použitím AI je spojena celá řada etických otázek. Byl by problém, kdybychom měli skvělou regulaci, ale na rozdíl od zbytku světa neuměli AI efektivně využít.“* S tímto výrokem souhlasil i profesor Michal Pěchouček. Ti, kteří nezvládnou AI vhodně využít, tak podle něj do budoucna znevýhodní své podniky i občany. Profesor jde ale ve svých úvahách ještě dál: *„Regulace nemusí být podle mě nutně brzda inovace, ale může být i její akcelerací. AI je momentálně dodávaná velmi malým množstvím bohatých technologických firem a regulace může například pomoc k tomu, že se tento oligopol rozbije.“*

Diskutovaná byla vedle Aktu o AI také směrnice NIS 2 o kybernetické bezpečnosti. Mnoho českých firem totiž aktuálně kritizuje, že její chystaná implementace jde nad rámec pravidel, které stanovila Evropská unie a bude pro ně přílišnou zátěží. Téměř všichni přítomní se ale shodli na tom, že v této rovině je lepší být přísnější. *„Žádný zákon není fér pro všechny, ale v dlouhodobém horizontu by neměl nikomu stranit. A ačkoliv to v komerčním světě nezní moc dobře, tak bezpečnost nemá cenovku. Tu buďto máte nebo ji nemáte,“* vysvětluje Bartoš.

Jaká je v současnosti četnost útoků na ty nejsnazší cíle, jednotlivce, přiblížil divákům diskuze výzkum, který Zlatá koruna připravila s agenturou IPSOS. Podle něj čelila téměř polovina Čechů v poslední době nějaké jeho formě, nejčastěji takzvanému phishingu. Pětina z nich dokonce přišla o finanční prostředky. *„Prototypem průměrné oběti kyberútoku v České republice je překvapivě muž v produktivním věku z Prahy nebo Středočeského kraje. Nejčastější hodina útoku je sedmá večer během svátku nebo víkendu, kdy lidé najednou otupí, a také v čase, kdy platíme daně a všichni jsou ve stresu,“* popsala svoje zkušenosti s kyberútoky z praxe COO Komerční banky Jitka Haubová. Podle ní bylo terčem útoku během loňského roku 70 tisíc jejich klientů a zhruba polovinu z nich se podařilo zvrátit díky detekčním systémům banky. V mezinárodním kontextu jsou ale tato čísla podle generálního ředitele Visa pro ČR, SR a Maďarsko Marcela Gajdoše pozitivní: *„Bydlím tu patnáct let a jsem velmi hrdý, že Česko patří mezi státy s nejmenším množstvím podvodů na počet transakcí. To je zrcadlem toho, že jsou tu společnosti a finanční sektory, které velmi dobře ví, co z umělé inteligence chtějí vytěžit a lidé se tu vzdělávají.“*

Na otázku, jak se máme chovat, abychom se nenapálili, odpovídá Leader AI Institutu společnosti Deloitte Jan Hejtmánek jednoznačně: *„Zodpovědně. Problém je, že děti každý rodič naučí, že se mají rozhlížet, než přejdou přes přechod, ale jak se chovat ve virtuálním světě, často vědí méně než ony.“* Podle Hejtmánka je pro spoustu lidí nepředstavitelné, jak těžko rozpoznatelné některé scamy dnes jsou. Podvodníci si ze střípků z našich sociálních sítí dokážou lehce poskládat, jakým způsobem k nám mají promlouvat a sestavit tak třeba email přesně nám na míru. Podle Marcela Gajdoše už dnes

kreativita podvodníků téměř nezná meze. Popisuje, že mezi nejnebezpečnější podvody současnosti patří takzvané romance scamy. Jejich oběťmi jsou nejčastěji ženy, které uvěří tomu, že člověk, který s nimi chatuje nebo telefonuje, potřebuje pomoci, a někdy tak v návalu emocí podvodníkovi zašlou i miliony korun.

Jakým způsobem vzdělávat o kyberbezpečnosti jednotlivé věkové kategorie bylo velkým tématem druhé části diskuze. Panelisté se shodli, že AI je tématem, o kterém se musí nutně dozvídat všichni občané, od dětí v mateřské školce až po důchodce. Na nejstarší generaci Ivan Bartoš aktuálně cílí originálně: *„Snažím se teď do digitálního vzdělávání zapojit šest tisíc knihoven, aby pomáhali těm, kteří nikomu, kromě svého knihovníka, nevěří.“* Podle docenta VŠE Pavla Hnáta je neustálé zabývání se etickými aspekty použití umělé inteligence ve školství sice důležité, ale trochu tato debata zastiňuje to nejdůležitější: tedy podporu mladých lidí, aby se naučili technologii co nejlépe využít. *„Jako zradu vnímám, že většina našich studentů je napřed, protože je pro ně technologie úplně přirozená, zatímco učitelé se musí teprve naučit jí důvěřovat.“*

To, v čem má česká společnost podle panelistů největší mezery je pochopení, že kyberbezpečnost už dávno není jen otázkou samotných technologií. Ochranné systémy jsou sice účinné, ale na čím dál sofistikovanější útoky samy nestačí. Nejlepší obranou je jejich spojení přímo s uživatelem. A právě proto je podle panelistů nutné se v oblasti AI stále vzdělávat. *„Cybersecurity je problém, který řeší technologie a člověk zároveň. Člověk vždy musí přispět a být součástí rozhodnutí a sám o tom přemýšlet,“* uzavírá profesor Pěchouček.

http://www.ceskenoviny.cz/tiskove/zpravy/bezpecnost-v-kybernetickem-svete-nad-kterou-se-musi-premyslet/2565717