Rizika kybernetické bezpečnosti, spojená s aplikací umělé inteligence v autonomních vozidlech

Zdroj – Tisková zpráva

Očekává se, že odstraněním nejčastější příčiny dopravních nehod, tj. lidské chyby, autonomní vozidla sníží dopravní nehody a úmrtí. Mohou však představovat zcela odlišný druh rizika pro řidiče, cestující a chodce.

Autonomní vozidla používají systémy umělé inteligence, které využívají techniky strojového učení ke sběru, analýze a přenosu dat, aby mohly činit rozhodnutí, že v běžných automobilech jsou přijímána lidmi. Tyto systémy, stejně jako všechny systémy IT, jsou zranitelné vůči útokům, které by mohly ohrozit řádné fungování vozidla.

Nová zpráva European Union Agency for Cybersecurity (ENISA) a Joint Research Centre (JRC) se zabývá kybernetickými riziky spojenými se vstupem Articifial Intelligence (AI) do autonomních vozidel, a poskytuje doporučení k jejich zmírnění. Hlavní motto: Výhody autonomního řízení nesmí být vyváženy bezpečnostními riziky.

Zranitelnost AI v autonomních vozidlech.

Systémy umělé inteligence autonomního vozidla pracují nepřetržitě, aby rozpoznaly dopravní značky a dopravní značení, detekovaly vozidla, odhadly jejich rychlost a plánovaly cestu vpřed. Kromě neúmyslných hrozeb, jako jsou náhlé poruchy, jsou tyto systémy citlivé na úmyslné útoky, jejichž specifickým cílem je zasahovat do systému AI a narušit funkce důležité z hlediska bezpečnosti.

Příkladem takových útoků je přidání barvy na silnici, aby se navigace zmýlila, nebo nálepky na stopce, aby se zabránilo jejímu rozpoznání. Tyto změny mohou vést k tomu, že systém AI nesprávně klasifikuje objekty, a následně k tomu, že se autonomní vozidlo bude chovat způsobem, který by mohl být nebezpečný.

Doporučení pro bezpečnější AI v autonomních vozidlech.

Aby se zlepšilo zabezpečení AI v autonomních vozidlech, zpráva obsahuje několik doporučení, jedním z nich je, že bezpečnostní hodnocení komponent AI se provádějí pravidelně po celou dobu jejich životního cyklu. Toto systematické ověřování modelů a dat AI je nezbytné k zajištění toho, aby se vozidlo vždy chovalo správně, když čelí neočekávaným situacím nebo škodlivým útokům.

Dalším doporučením je, že nepřetržité procesy hodnocení rizik podporované zpravodajstvím o hrozbách by mohly umožnit identifikaci potenciálních rizik umělé inteligence a vznikajících hrozeb souvisejících se zaváděním umělé inteligence v autonomním řízení. Správné zásady zabezpečení AI a kultura zabezpečení AI by měly řídit celý dodavatelský řetězec pro automobilový průmysl.

Automobilový průmysl by měl pro vývoj a nasazení funkcí umělé inteligence přijmout koncepci zabezpečení typu „design by design “, kde se kybernetická bezpečnost od počátku stává ústředním prvkem digitálního designu. Nakonec je důležité, aby automobilový průmysl zvýšil svou úroveň připravenosti a posílil své schopnosti reakce na incidenty při řešení vznikajících problémů v oblasti kybernetické bezpečnosti souvisejících s umělou inteligencí.

Blíže k obsahu vlastní zprávy:

Pokroky v umělé inteligenci otevřely zcela nové příležitosti v mnoha oblastech propojené digitální společnosti. Možnost automatizace velkých částí každodenních činností až dosud jako mimo dosah výpočetních strojů, nabízí nové pohledy na řešení mnoha výzev, kterým lidé čelí. V odvětví dopravy hraje AI klíčovou roli při vývoji nových generace automobilů, které budou poskytovat autonomní a poloautonomní služby řízení cestujícím a umožnit vysokou úroveň automatizace se hmatatelnými výhodami, pokud jde o úmrtnost na silnicích, dopravní zácpy nebo možnosti mobility. V tomto ohledu se AI používá jako prostředek ke zdokonalování zajišťování služeb a nabídka bezpečnější a bezpečnější jízdní podmínky. Zároveň však tam jsou bezpečnostní důsledky AI na celý ekosystém digitálních produktů a služeb. AI umožňuje nové případy použití, kdy kybernetické dopady překračují bariéru mezi digitálním a fyzickým světem a mohou přejít do vážných bezpečnostních problémů. Automobilový průmysl představuje vysoce rizikovou doménu přímo ovlivněnou riziky s nimi spojenými problémy kybernetické bezpečnosti. Automobilová bezpečnost ve skutečnosti je úzce souvisí s bezpečností: kybernetické útoky mohou způsobit bezpečnost potenciální problémy a škody ve fyzickém světě ve velkém měřítku. To vše představuje důvod pro zaměření úsilí na zmírnění rizika v tomto sektoru.

Tato zpráva si klade za cíl poskytnout poznatky o těchto výzvách v oblasti kybernetické bezpečnosti, konkrétně souvisejících s využíváním technik AI v autonomních vozidlech.

Hlavní požadavky do budoucnosti:

- Zabezpečení dodavatelského řetězce AI v automobilovém průmyslu.
- Systematické bezpečnostní ověřování modelů AI a dat.
- Kybernetické bezpečnostní procesy a kontroly AI techniky autonomního řízení
- Zvýšení schopnosti připravenosti a reakce na bezpečnostní incidenty.
- Zvýšení kapacit a odbornosti v oblasti AI kybernetické bezpečnosti pro automobilové systémy.