

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **72** ze dne **18.6.2024**

AI v oblasti kyberbezpečnosti: Příležitost i hrozba

Generativní umělá inteligence se stále častěji stává plnohodnotným pracovním nástrojem. Dvě třetiny podniků v loňském roce uvedly, že ji již začínají využívat, a pouhá 3 % ji zavést neplánují. Z toho vyplývají nové výzvy nejen pro šéfy informační bezpečnosti ve firmách, ale pro oblast kybernetické bezpečnosti jako takovou.

Z hlediska kybernetické bezpečnosti se umělá inteligence stala dvojsečnou zbraní. Na jedné straně dala kyberzločincům do ruky možnosti, které si donedávna jen málokdo dokázal vůbec představit. Na druhou stranu však má potenciál vyrovnat síly i vůči silicím hrozbám – kybernetičtí obránci mohou využít AI k inteligentní automatizaci i v obranných strategiích.

Nové možnosti kyberzločinu

Umělá inteligence dává kyberzločincům do rukou zcela nové nástroje i schopnosti. Pravidla, která zaměstnanci i veřejnost používali k identifikaci podvodů, přestávají platit. Generativní umělá inteligence může výrazně zdokonalit cílené phishingové útoky, protože dokáže lépe formulovat zprávy bez pravopisných chyb nebo neohrabané gramatiky, jak je pro podvodné e-maily typické. Podaří-li se útočníkovi získat adresář oběti, může také převzít obsah e-mailu a použít jej k vygenerování e-mailů na míru, které odpovídají stylu a tématům konverzací napadeného uživatele s jednotlivými adresáty. Jistotu už dnes nepředstavuje ani telefonní nebo videohovor, zločinci začali využívat hlasové a video napodobeniny údajného odesílatele vygenerované umělou inteligencí a odpovědi generované konverzačními roboty. Snadno se tak může stát, že zaměstnanec pod dojmem, že mluví se svým nadřízeným, převede velkou finanční částku na účet útočníka.

Potenciální kybernetický útočník dnes už díky generativní umělé inteligenci nepotřebuje žádné programátorské dovednosti, k psaní malwaru může použít nástroje umělé inteligence s rozsáhlými jazyko-vý-mi modely. Umělá inteligence se také používá k rychlému napadení zranitelností softwaru, jakmile jsou veřejně známé. Útočníci mají šanci takové zranitelnosti zneužít rychleji, než mnozí zákazníci dokáží aplikovat záplaty nebo aktualizace od poskytovatele softwaru.

Jak se za pomoci AI bránit?

Kybernetičtí zločinci málokdy uspějí hned při prvním útoku na cíl – a to ani s pomocí umělé inteligence, ale spoléhají na to, že jejich neúspěšné útoky zapadnou v množství výstrah, které dennodenně zaplavují bezpečnostní operační centrum podniku. Umělá inteligence pomáhá odhalit anomální aktivity, určit, za kterými anomáliemi stojí reálné útoky a v reálném čase zajistit odpovídající reakci. Umělá inteligence a strojové učení jsou založené na datech – a čím více dat mají k dispozici pro trénink a práci, tím jsou efektivnější. A ti, kdo provozují a chrání podnikové prostředí, mívají taková data k dispozici spíše než ti, kdo se snaží do sítě proniknout. Zatímco například u phishingu mají výhodu útočníci, v tomto případě jsou na vítězné straně obránci.

Podrobně zmapovat rozsáhlá digitální prostředí firem a organizací a najít v nich potenciální slabá místa je často velmi obtížné. Díky AI a narůstajícímu využití kyberbezpečnostní mesh architektury je možné proměnit tuto nevýhodu ve výhodu. Senzory propojené jednotnou architekturou umožňují provozovatelům a obráncům sítí v reálném čase generovat data, která dokáže stále výkonnější umělá inteligence a strojové učení v reálném čase vyhodnocovat.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **72** ze dne **18.6.2024**

Rizika využití AI v rámci firem

Jakkoli je AI z hlediska informační bezpečnosti přínosem, její využití na pracovišti přináší nové komplikace. Jedním z největších problémů je, že data obsažená v dotazech pro generativní umělou inteligenci se stávají součástí datové sady jazykového modelu, který daná AI využívá. Snadno se tak mohou například zveřejnit citlivé firemní informace. Mezi další časté problémy patří porušování autorských práv, odhalování informací umožňujících osobní identifikaci, ne-vě-do-mé užívání zkreslených nebo nevhodných dat a tzv. „halucinace“ umělé inteligence, jak se označuje uvěřitelně formulovaný, ale zcela chybný výstup. Při využívání generativní umělé inteligence je na místě opatrnost, bohužel zaměstnanci, kteří experimentují s tímto nástrojem v soukromí, si navykli využívat jej i na pracovišti a ne-do-mýš-lí důsledky. Generativní umělá inteligence se tak stala nejnovější formou stínového IT, se kterou se musí ČISO a CIO vypořádat.

Inovace založené na umělé inteligenci se odehrávají v celém technologickém prostředí a je na podnicích, aby je využily. Mezi kybernetickými útočníky a obránci probíhají závody ve zbrojení, jak dopadnou, ukáže teprve budoucnost. Obránci ale už teď mají nástroje i potenciál k tomu stát se vítěznou stranou, je však třeba zvolit vhodné nástroje i strategii.

Zdroj: AVcentrum ČR