Doktorand FEL ČVUT uspěl s AI ochranou proti kyberútočníkům. Projekt vznikající v Centru umělé inteligence míří na trh

30.6.2026 - | Fakulta elektrotechnická ČVUT v Praze

Jak mohou organizace odhalit, zdržet a zmást útočníky, kteří už pronikli do jejich sítě?

Právě na tuto výzvu odpovídá projekt Decor, za kterým stojí doktorand FEL ČVUT Muris Sladić a dr. Sebastian Garcia ze Stratosphere Lab, výzkumné skupiny Centra umělé inteligence FEL ČVUT. Decor využívá umělou inteligenci a principy kybernetické klamné obrany k odhalování, matení a zadržování útočníků, kteří se již dostali do podnikové sítě. Obráncům tak poskytuje včasnější přehled o aktivitách útočníků a více času na reakci. Projekt zvítězil v programu Get Spin-off/Start-up Ready!, který pomáhá studentům a výzkumníkům proměňovat výzkumné nápady v budoucí startupy a spin-offy.

Program Get Spin-off/Start-up Ready!, organizovaný ČVUT Technology Transfer, propojuje studenty, doktorandy a výzkumníky s mentory z byznysu, investory a odborníky na komercializaci technologií. Do prvního ročníku postoupilo 16 účastníků z různých fakult ČVUT, přičemž hned šest studentů bylo z Fakulty elektrotechnické ČVUT.

Vítězný projekt Decor vznikl na pomezí špičkového výzkumu v oblasti kyberbezpečnosti a praktických potřeb firem. Za jeho vývojem stojí Muris Sladić, doktorand katedry počítačů FEL ČVUT, a Sebastian Garcia, vedoucí Stratosphere Lab. Tato sedmnáctičlenná výzkumná skupina působí v rámci Centra umělé inteligence FEL ČVUT a dlouhodobě se zaměřuje na výzkum kyberbezpečnosti, umělé inteligence a síťových technologií.

Projekt Decor reaguje na stále častější situace, kdy útočník získá přístupové údaje zaměstnance a dostane se dovnitř podnikové sítě, aniž by vyvolal podezření tradičních bezpečnostních systémů.

„Současné bezpečnostní nástroje jsou velmi dobré v obraně proti útokům zvenčí. Problém nastává ve chvíli, kdy se útočník dostane dovnitř sítě pomocí ukradených přihlašovacích údajů. Naším cílem je vytvořit prostředí, které vypadá jako skutečná infrastruktura firmy, ale ve skutečnosti jde o řízenou past, která útočníka odhalí a zadrží," vysvětluje Muris Sladić.

Když se vetřelec ocitne v pasti

Technologie využívá princip takzvané kybernetické klamné obrany (cyber deception). Místo pouhé detekce útoku vytváří věrohodné falešné služby a systémy, se kterými útočník interaguje v domnění, že se pohybuje v reálném prostředí organizace. Obránci tak získávají cenný čas na reakci.

„V tradičních konfliktech je klamání protivníka součástí obrany už tisíce let. V kyberbezpečnosti se tento přístup teprve začíná prosazovat. Naším cílem je pomoci organizacím převzít kontrolu nad tím, co útočník vidí a čemu věří," říká Sebastian Garcia, vedoucí Stratosphere Lab.

Podle něj může právě čas rozhodovat o tom, zda útok skončí drobným incidentem, nebo milionovými škodami. „Pokud dokážeme útočníka zaměstnat na dvě nebo tři hodiny v řízeném prostředí, může to být rozdíl mezi úspěšnou obranou a rozsáhlým únikem dat."

Významnou roli v celém řešení hraje umělá inteligence. Zatímco AI pomáhá obráncům vytvářet

přesvědčivé klamné prostředí, stále častěji ji využívají také samotní útočníci.

„Umělá inteligence dnes výrazně zvyšuje možnosti obránců i útočníků. Útoky jsou rychlejší a sofistikovanější než dříve. Právě proto věříme, že AI musí být součástí obrany – lidské týmy samy už nedokážou reagovat dostatečně rychle na vše, co se v sítích odehrává," doplňuje Garcia.

Od výzkumu k produktu

Projekt Decor vychází z výzkumu, kterému se Muris Sladić věnuje již od diplomové práce a následně během doktorského studia. První verze řešení vznikaly jako jednotlivé AI honeypoty – falešné služby určené k odhalování útočníků. Postupně se však rozrostly do komplexního systému, který lze nasadit ve firemním prostředí.

V současnosti tým dokončuje takzvaný minimální životaschopný produkt (MVP) a jedná s potenciálními zákazníky o pilotním nasazení. „Technologie už funguje a prošla testováním jak v laboratorních podmínkách, tak v omezeném reálném prostředí. Teď se soustředíme na to, aby byla připravena pro nasazení ve firmách a splňovala vysoké požadavky na bezpečnost a důvěryhodnost," říká Sladić.

Podle něj je dnes největší výzvou získání důvěry zákazníků. Samotná technologie již funguje, ale firmy musí mít jistotu, že nové bezpečnostní řešení nebude představovat další riziko. Právě proto tým navrhl systém tak, aby nevyžadoval instalaci dodatečného hardwaru ani softwarových agentů uvnitř chráněné organizace. První pilotní nasazení a ověřování v produkčních prostředích by podle týmu mohla začít během několika následujících měsíců.

Program, který otevírá dveře do světa startupů

K rozvoji projektu významně přispěla právě účast v programu Get Spin-off/Start-up Ready!, který účastníkům nabízí mentoring zkušených podnikatelů, praktické workshopy i individuální konzultace.

„Jako počítačový vědec jsem měl omezené zkušenosti s obchodní stránkou věci. Program mi pomohl pochopit, jak přemýšlet o zákaznících, obchodním modelu nebo ověřování tržního potenciálu. Největší přínos pro mě představovala spolupráce s mentory z byznysu, kteří nám pomohli podívat se na projekt z úplně jiné perspektivy," říká Muris Sladić.

Pozitivně hodnotí program také dr. Sebastian Garcia. „Na ČVUT je vidět skutečná snaha pomáhat výzkumníkům a studentům při zakládání startupů a spin-offů. Kolem programu se podařilo soustředit zkušené mentory a odborníky, kteří dokážou pomoci zorientovat se ve světě podnikání a komercializace výzkumu."

Přihlášky do dalšího běhu programu Get Spin-off/Start-up Ready! jsou otevřeny do 8. září 2026. Program je určen studentům, doktorandům, postdoktorandům i výzkumníkům, kteří chtějí ověřit komerční potenciál svých nápadů a výzkumných výsledků.

„Pokud máte pocit, že váš výzkum nebo projekt může mít reálný dopad v praxi, určitě to zkuste. V nejhorším případě získáte nový pohled na svou práci. V tom nejlepším můžete zjistit, že máte základ budoucího startupu," shrnuje Muris Sladić svou zkušenost z účasti v programu.

https://fel.cvut.cz/cs/aktualne/novinky/84636-doktorand-fel-cvut-uspel-s-ai-ochranou-proti-kyberutocnikum-projekt-vznikajici-v-centru-umele-inteligence-miri-na-trh