HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
28. – 30. JÚNA 2024

Odborná spolupráca
NBÚ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Môžete ju zbožňovať. Môže vás desiť. AI

Digitálny priestor je zaplnený informáciami, ktoré sa stávajú „potravou" umelej inteligencie. FOTO: DREAMSTIME

TÉMA

Umelá inteligencia sa vybrala rôznymi cestami. Na jednej nájdete špičkové riešenia vrátane bezpečnosti, na inej halucinácie.

Skončila sa éra „vynorovania" kybernetických bezpečnostných špecialistov a začal sa boom špecialistov na umelú inteligenciu.

Ironický postreh je od kyberbezpečnostného profesionála Romana Čupku, napísal ho ešte v roku 2022 a stále si za ním stojí: „Rozmach tejto ďalšej éry digitálnej transformácie je skutočne robustný. Cítiť to nielen na akciových trhoch, ale aj v bežnom živote."

Fakty nepustia

Aplikácie na báze umelej inteligencie používa čoraz širšie spektrum používateľov. Peter Bakonyi zo spoločnosti Aliter Technologies sa venuje umelej inteligencii už šesť rokov a v praxi sa stretáva s jej rastúcou akceptáciou. „Využitie AI má obrovský potenciál v každej oblasti. Zatiaľ sa však ľudia iba učia efektívne ju používať."

Podľa jeho skúseností sa umelá inteligencia vo firmách najviac uplatňuje v programátorskej oblasti. „Generovanie zdrojového kódu, ladenie alebo optimalizácia sú len niektoré príklady, ako sa AI aplikuje v každodenných úlohách," vysvetľuje Peter Bakonyi a zároveň verí, že ak by sa zlepšila osveta, padlo by mnoho ďalších bariér.

Napríklad vytvorenie kvalitného modelu na spracovanie textu je ešte stále drahá záležitosť. A pritom niekedy je potrebné iba trochu zmeniť existujúcu aplikáciu, aby splnila požadovanú úlohu.

Posun je dramatický

V zdravotníctve umelá inteligencia výrazne zlepšila diagnostiku a personalizovanú starostlivosť. V marketingu poháňa chatbotov a virtuálnych asistentov, logistika sa preberá do zlatej éry. Technologické inovácie umožnili AI systémom ešte efektívnejšie spracovávať a analyzovať veľké množstvá dát.

Umelá inteligencia pomáha dokonca aj pri takých ťažkých úlohách, ako je detekcia a prevencia kybernetických útokov v reálnom čase. Metódy pokročilých algoritmov dokážu analyzovať obrovské množstvá dát, identifikovať anomálie a potenciálne hrozby skôr, než spôsobia škodu.

Niet cesty späť

„Vzhľadom na to, že útoky sú čoraz sofistikovanejšie a tradičné metódy ochrany zlyhávajú, je postupné nasadzovanie a používanie technológií s podporou AI viac-menej nevyhnutné," hovorí Jozef Bálint zo spoločnosti Alison Slovakia.

V kyberbezpečnosti sa hrá o čas, takže moderné riešenia už majú okamžitý prístup k stovkám zdrojov, dokážu analyzovať tisícku rôznych dátových formátov a súčasne využívajú aktuálne reporty zo senzorov sieťových zariadení.

Po dňoch a nociach pred obrazovkou počítača a po čítaní alertov sa však Jozef Bálint hlási k výroku – umelá inteligencia je inteligentná iba natoľko, akí boli inteligentní tvorcovia daného algoritmu.

Detaily robia rozdiel

S využitím veľkých jazykových modelov experimentujú aj kyberbezpečnostní profesionáli v slovenskej jednotke CERT. „Aby použitie umelej inteligencie malo zmysel, model musí byť dobre natrénovaný," upozorňuje Milan Pikula, riaditeľ SK-CERT. Takže môžeme nechať AI, nech hľadá zlo v systéme a hlási incidenty a navrhuje riešenia, ale bez človeka to ešte stále nebude mať hlavu a pätu.

Umelá inteligencia pozná celý internet, ale neberie do úvahy lokálny kontext v organizácii. V kyberbezpečnosti preto ešte dlho budú ľudia, ktorí si odporúčanie prečítajú a posúdia ich v kontexte monitorovaného prostredia.

Snaživá viac, ako treba

S príchodom AI aplikácií ožilo slovo „halucinácia". Predstavte si to ako na pohovore, kde dostaneme otázku, na ktorú nevieme odpovedať. Tak si niečo vymyslíme, aby sme neboli ticho, a toto isté robí aj umelá inteligencia!

AI nástroje niekedy podajú informáciu natoľko sugestívne, že ju nespochybňujeme a neoverujeme, a presne to sa nám môže vypomstiť. V horších prípadoch to môže byť zdrojom dezinformácií.

> UMELÁ INTELIGENCIA JE INTELIGENTNÁ IBA NATOĽKO, AKÍ BOLI INTELIGENTNÍ TVORCOVIA DANÉHO ALGORITMU.
>
> **Jozef Bálint,** špecialista kybernetickej bezpečnosti Alison Slovakia

Halucinácie a fabulácie modelov sa postupne znižujú, ale závisí to aj od toho, o aký typ AI ide. Na generovanie textu napríklad už existujú postupy, aby bol výstup AI z konkrétnych zdrojov, čím sa znižuje riziko halucinácií.

Čo trápi profesionálov

Okrem spomínaných pozitívnych prínosov pri diagnostike pacientov, úpravách a tvorbe programátorských kódov či rýchlejšej analýze kyberhrozieb upozorňuje Roman Čupka aj na tú temnejšiu stránku uplatnenia umelej inteligencie.

Už od roku 2016 je znateľný vplyv tejto technológie pri ovplyvňovaní politických súbojov v demokratických voľbách. Odvtedy sa umelá inteligencia dostala takmer do každej sociálnej siete a začína veľmi jednoducho meniť správanie ľudí.

Šikovní jednotlivci a marketéri dokážu využiť dátový a jazykový model so zacielením na tie najnižšie pudy ľudskej bytosti, ako sú strach či žiadostivosť.

Legislatívny semafor

Mnohé organizácie a inštitúcie si negatívny dosah umelej inteligencie uvedomujú a presadzujú smernice a národné regulácie, aby vyhliadky čo najviac zbrzdili.

V minulom roku predstavila Európska únia ako prvá na svete dohodu o pravidlách pre umelú inteligenciu. Cieľom je, aby boli AI systémy uvádzané na trh bezpečné a rešpektovali základné práva a hodnoty Únie. Rovnako však Únia vyzýva na investície a inovácie v tejto oblasti.

Zdravý sedliacky rozum

Ľudia žijúci v bohatších ekonomikách vnímajú produkty a služby využívajúce umelú inteligenciu menej pozitívne. Odborníci predpokladajú, že to súvisí s kritickým myslením a emocionálnym kvocientom.

V súčasnosti radi a často využívame nástroje, ktoré nám šetria čas. No stále zostáva dôležité prekontrolovať si výsledky a uvedomiť prípadné dosahy. Na pravidle „zdravého rozumu" sa vzácne zhodujú profesionáli z oblasti umelej inteligencie aj kybernetickej bezpečnosti.

POPULÁRNE VOĽNE DOSTUPNÉ AI APLIKÁCIE

ChatGPT
AI nástroj na generovanie textu, užitočný pre rôzne aplikácie zákazníckeho servisu a tvorby obsahu

Google Gemini
AI chatbot, ktorý sa bezproblémovo integruje s nástrojmi Google, ako sú Mapy, YouTube a Workspace

Microsoft Copilot
AI asistent zabudovaný do nástrojov Microsoftu, využíva architektúru GPT-4 na poskytovanie pokročilých funkcií pre používateľov

Claude
Ponúka širokú škálu spracovania textu a hlasu a prácu s dokumentmi, vhodný na profesionálne použitie

TensorFlow

PyTorch
Open-source rámce na strojové a hlboké učenie, používané v akademickom aj priemyselnom prostredí na vývoj AI modelov a aplikácií

PhotoDirector

PowerDirector
Pokročilé AI funkcie na úpravu fotografií a videí, sú dostupné na použitie s voliteľnými prémiovými funkciami pre začiatočníkov aj profesionálov

Stable Diffusion
Open-source model, ktorý dokáže generovať podrobné vizuály z textových opisov

Lumen5
AI nástroj na tvorbu videí, ideálny pre marketingový a sociálny mediálny obsah

Špeciálnu prílohu podporujú

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 28. – 30. JÚNA 2024

Z týchto odpovedí vás obídu mdloby

ANKETA

Komunita kybernetickej bezpečnosti dostala zadanie: Napísať phishingovú správu, ktorá by vo vašom segmente, kde pracujete, mohla byť veľmi účinná a naviedla by príjemcu na „kliknutie“. Môžete použiť AI aplikáciu, vlastnú kreativitu, alebo oboje.

Napísať odpoveď alebo mlčať? Časť respondentov sa rozhodla mlčať. Časť vyjadrila obavy až pobúrenie. Časť respondentov však neváhala pomenovať neduhy, nebezpečenstvo a hrozby v plnej sile a neľútostne ukázať na naše slabosti. Tieto anketové odpovede nie sú ani jednoduché, ani jednoznačné. Ak začnú diskusiu, alebo vás preberú z ľahostajnosti, otázka splnila účel. Posúďte sami.

Tibor Szabo,
vedúci Oddelenia auditu IT, Všeobecná úverová banka

Chcel som využiť umelú inteligenciu, ale jej „právne povedomie“ je už vysoko. Odmietla ma pre nezákonnosť otázky. Tak skúsim sám: „Vážený klient, z dôvodu nárastu množstva phishingových útokov Vás chceme z dôvodu Vašej ochrany požiadať, aby ste čo najskôr prostredníctvom priloženého linku overili zostatok na Vašom účte. V prípade nezrovnalosti nás obratom kontaktujte. Naša povinnosť je chrániť Vás.“ A poslať cez SMS aj s menom banky.

Timea Tomčová,
manažérka informačnej bezpečnosti, Poisťovňa Union

Z mojich skúseností práve tie menej sofistikované phishingy takmer vždy zafungujú. Napríklad emaily informujúce o novom zamestnaneckom benefite, výhre, plánovanom teambuildingu, konferencii alebo odstávke vody v budove. Naletieť môže ktokoľvek, netreba mať ilúzie, že mne sa to nestane. Preto je dôležité kontinuálne sa vzdelávať, vedieť rozoznať základné znaky phishingu a osvojiť si to, ako správne postupovať v prípade, ak sa už človeku podarí naletieť.

Roman Čupka,
hlavný konzultant, Progress a CSO Istrosec

Keď verejne dostupnej umelej inteligencii priamo zadáte, aby vytvorila cielenú kampaň na špecialistu v oblasti kybernetickej bezpečnosti, nepomôže vám. Je to pre ňu „amorálne“. Stačí si s ňou však trocha pohovoriť a zrazu je prístupná vám pomôcť. Mne osobne na to stačili štyri „promty“ a dostal som použiteľný príklad phishingového emailu, ktorý cieli na analytika Centra bezpečnostných operácií (SOC).

Marián Trizuliak,
architekt kybernetickej bezpečnosti, Západoslovenská distribučná

Platí pravidlo – v správnom čase správna téma, a používatelia sa chytia. Aj tí najskúsenejší a obozretní stratia obozretnosť.

Predmet: Aliexpress – tvoja objednávka

Telo správy:
Ďakujeme, XY, za tvoju objednávku v obchode AliExpress. Pre zaslanie dokladu/faktúru k tvojej nedávnej objednávke klikaj čo najskôr „tu“.

Predmet: Darček pre futbalomaniakov od AlzZáka

Telo správy:
Už je to tu! Všetci futbaloví fanúšikovia sa ponáhľajú, aby stihli nakúpiť výbavu majstrov sveta! Nakupuj ešte dnes na nasledujúcom „odkaze“ a získaš dodatočnú zľavu 15 %!!!

Predmet: Odkaz v Teams hlasovej schránke od používateľa Jano

Telo správy:
Ahoj, používateľ Teamsu, počas tvojej neprítomnosti ti používateľ Jano zanechal v Teams hlasovej schránke odkaz na stiahnutie. Pre vypočutie odkazu použi administrátorské práva!

Tomáš Vobruba,
vedúci bezpečnostný inžinier, Check Point Software Technologies

Tak minútu mi trvalo, kým som zadal aplikácii svoju profesiu, meno syna, názov streamovacej služby a požiadavku, aby napísala ukážku phishingového mailu. Po pár minútach optimalizácie som mal k dispozícii sugestívny mail vrátane predmetu, mena operátorky, vyjadrenia starostlivosti aj naprogramovanú verziu s logom streamovacej služby. Tento HTML kód vytvorí e-mail s grafickým logom a textom. Logo je vložené pomocou URL odkazu na obrázok na Wikipedii, čo je bežná prax, a zaisťuje, že obrázok sa správne načíta pri zobrazení e-mailu. Phishing je taký dobrý, že vám ho nemôžem ukázať.

Róbert Mramúch,
manažér kybernetickej bezpečnosti, MH Teplárenský holding

Možno by stačila správa s nejakým ľúbivým textom, napríklad: „Od júla klesne cena tepla vo všetkých mestách o 90 percent.“ A pod tento text umiestniť veľké tlačidlo „Nahlásiť spam“. Samozrejme, že podvodný link by bol zakomponovaný v tom tlačidle...

Andrej Žucha,
generálny riaditeľ, ALISON Slovakia

„Kolegyne a kolegovia, tak ako každý mesiac sa Vám chcem prihovoriť s tým, čo je nové v našej spoločnosti. Pripravili sme pre Vás nové benefity na toto leto. Vybrať si ich môžete prostredníctvom tohto linku. A, samozrejme, nezabudnite si aj pozrieť, čo je nové vo sfére kybernetickej bezpečnosti v prílohe HN na tomto linku.“

Ivan Makatura,
generálny riaditeľ, Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Text phishingovej správy je typicky prispôsobený jej účelu. My sme akreditovaní na poskytovanie grantov z priamo riadených fondov EÚ a tvoríme európsku komunitu kyberbezpečnosti. Ak by som teda mal pomocou sociálneho inžinierstva presvedčiť niekoho, aby si klikol na web kyberkomunita.sk a podal si žiadosť o podporu projektu, na to stačí aj náš newsletter. V podstate je to spear phishing.

Marek Madžo,
technický riaditeľ, centrum kybernetickej bezpečnosti void SOC

Toto školenie ti pomôže rozpoznať a vyhnúť sa phishingovým útokom, ktoré by mohli ohroziť našu spoločnosť.

Aby sme zapojili všetkých zamestnancov a zvýšili tak našu kolektívnu informovanosť o kybernetickej bezpečnosti, prosím, potvrď svoju účasť kliknutím na odkaz nižšie:
Klikni sem pre potvrdenie tvojej účasti

Ďakujeme za tvoju rýchlu odpoveď a spoluprácu. Spoločne dokážeme udržať našu sieť bezpečnú.

S pozdravom,
[Vaše meno]
IT bezpečnostný tím
[Vaša spoločnosť]

Peter Bukovinsky,
šéf IT bezpečnosti Eviden Slovensko

Takmer všetky formy nešpecifického spôsobu nachytania tu už boli. Dnes sú účinné špecifické podvrhy s dobre falzifikovaným odosielateľom z firmy a zamerané na znalosť prostredia. Odhadujem, že z nešpecifických foriem phishingu by mohol byť relatívne účinný takýto scenár:

From: dobre@vam-tak.sk

Subject: Test phishingu – NIKDE NEKLIKAŤ!!!

Dobrý deň vám prajeme,

Toto je test phishingu – nie že sa necháte nachytať, aby ste klikli na túto čertovinu.

Ak sa necháte nachytať, dobre vám tak, a ešte k tomu:

Budete musieť absolvovať základné školenie o bezpečnosti;

Budete musieť absolvovať špeciálne školenie o phishingu;

Budete nahlásení na personálne oddelenie a za trest týždeň utierať zem pod pisoármi.

Ďakujeme, že ste neklikli ani na jeden z podvrhnutých linkov!

Ivan Kopáčik,
bezpečnostný expert, Gordias

Ako formu rafinovaného „proxy-phishingu“ vnímam túto anketovú otázku. A keďže sa nemienim stavať do úlohy phishingového bota a generovať podklady pre potenciálne phishingové útoky, na otázku priamo neodpoviem.:) Ale som zvedavý, koľko účastníkov ankety podľahne tejto phishingovej otázke, ktorá je zároveň testom.

Katarína Kročková,
odborníčka na ochranu osobných údajov, Kročka & Partners

Poskytovanie návodov na zlepšenie phishingových správ je zlý nápad. Odpoveď na otázku, teda phishingová správa vytvorená odborníkom na kybernetickú bezpečnosť, môže byť zneužitá na podvodné aktivity a ohroziť bezpečnosť osobných a firemných údajov. Mojou profesionálnou povinnosťou je presný opak – chrániť tieto údaje a udržiavať vysokú úroveň kybernetickej bezpečnosti.

Jakub Berthoty,
advokát, Dagital Legal

„Pre GDPR projekt za 39 eur kliknite sem.“

Daniel Chromek,
riaditeľ informačnej bezpečnosti, ESET

Pracovníci v oblasti informačnej bezpečnosti, samozrejme, na phishingové emaily neklikajú.:) Pekná príležitosť na phishing sa však otvorila na americkom trhu: Milý, vzhľadom na zákaz produktov Kaspersky na americkom trhu potrebujeme zmigrovať naše antivírusové prostredie na iného vendora. Prosíme Vás o nacenenie položiek v prílohe. S pozdravom.

Róbert Runčák,
partner pre technologické služby, Skupina CYLLIUM

Vybral som na phishing komerčný nástroj a upravil som aj vizuál. Všetky linky sú „živé“. Neklikajte.

Michal Srnec,
vedúci oddelenia informačnej bezpečnosti, Aliter Technologies

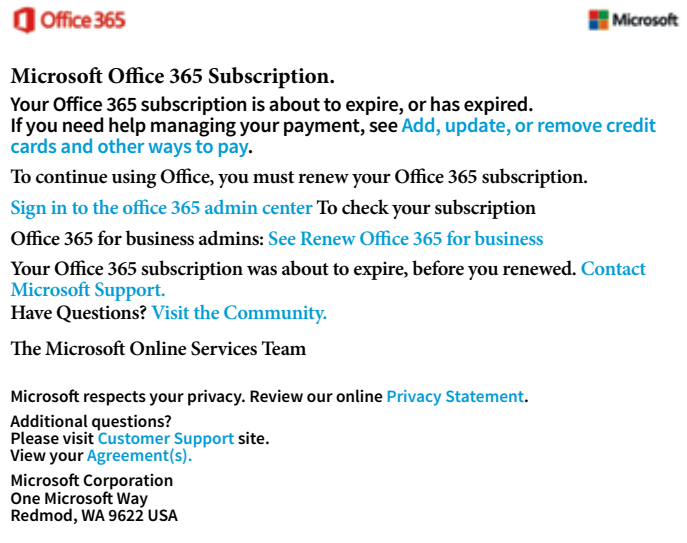
Vytvoriť účinný phishingový email pre profesionálov v oblasti informačných technológií by bol (ako pevne verím) oriešok. Vzhľadom na to, že poznajú typické znaky phishingového emailu (opätovne, ako pevne verím), by som sa pokúsil naformulovať „na prvý pohľad jasne identifikovateľný phishingový email s dokonca zlou slovenčinou“, pričom podvodný link by som skryl do odkazu „Report this message“.

Pavol Vrabec,
manažér kybernetickej bezpečnosti, Univerzitná nemocnica Martin

Ak by som mal zamerať phishing na náš segment a našu nemocnicu, tak by súvisel s aktuálnou výstavbou novej nemocnice. Na vytvorenie emailu som použil Chat GPT: „S radosťou Vám oznamujeme, že výstavba novej nemocnice v Martine je v plnom prúde, a máme pre Vás dôležité informácie týkajúce sa tohto projektu. V rámci príprav na otvorenie novej nemocnice sme zriadili interný portál, kde nájdete všetky potrebné informácie, aktualizácie a dôležité dokumenty súvisiace s týmto projektom. Aby ste mali prístup k týmto informáciám, je potrebné sa prihlásiť na tento nový portál.“

Marek Zeman,
vedúci oddelenia bezpečnosti informačných systémov, Tatra banka

Chcete zbohatnúť ako naši politici? Mať sa dobre, celé dni si počítať majetok, o nič sa nestarať? Potrebujete: 500 eur na karte a klik na link! S pozdravom

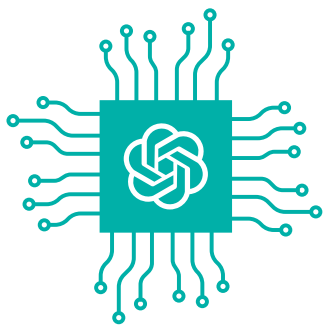


HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 28. – 30. JÚNA 2024

Všetko, čo ste sa vždy chceli opýtať

FAKTY

Hovorí sa o nej, píše, diskutuje, plní strany bulváru a vedeckých publikácií. Pozrite si fakty a čísla, ako hodnotia slovenskí odborníci povedomie po necelých dvoch rokoch.



Momentálne najpoužívanejší voľne dostupný systém umelej inteligencie je **ChatGPT produkt spoločnosti OpenAI.** Tu sú aktuálne fakty.

prvý
milión používateľov
získal ChatGPT už päť dní od vydania v roku 2022

viac ako 180 miliónov používateľov
denne kladie rôzne otázky alebo sa inšpiruje

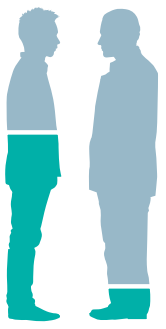
13,79 percenta používateľov
je zo Spojených štátov amerických

117 miliónov parametrov
mal model **ChatGPT pri prvej verzii**

117 biliónov parametrov
má aktuálna verzia **GPT-4.o**

Parametre si môžeme predstaviť ako doplnkové vybavenie auta – čím viac ich máme, tým viac funkcionalít má naše auto. V prípade AI ide o schopnosť učiť sa a riešiť komplexnejšie úlohy.

menej než 35 rokov
má až 59 % aktívnych používateľov



viac než 55 rokov
má iba 9 % používateľov

Najčastejšie okruhy otázok sú informácie ohľadne programovania, generovanie marketingového obsahu alebo otázky o hrách.

Percento chybovosti sa pohybuje medzi 3 až 30 %. Je to však závislé aj od správnej formulácie otázky. Odpovede, ktoré vám umelá inteligencia poskytne, si treba overovať, pretože niekedy sa aj mýli.

Ak nie sme spokojní s odpoveďou, treba trochu zmeniť otázku alebo si znovu vyžiadať odpoveď, ak sa nám zdá, že aplikácia nám vracia nesprávne informácie.

Spracoval:
Peter Bakonyi, Aliter Technologies

Odporúčanie:
Nástroje AI sú voľne dostupné a je možné ich využívať aj zadarmo. Pomocou textového okna sa môžeme s AI porozprávať na rozumnej úrovni, či už chceme nový recept alebo potrebujeme vzorec na výpočet daní.

TOP 5 OTÁZOK

V posledných mesiacoch sme sa s kolegami zúčastnili na viacerých odborných podujatiach, na ktorých sme na pódiách i mimo nich diskutovali o aktuálnych témach súvisiacich s umelou inteligenciou i digitálnou bezpečnosťou.

Tieto diskusie s manažérmi, IT špecialistami i laikmi nám poskytli určitý nadhľad – zistili sme, že mnohé organizácie dnes vnímajú tie isté otázky ako najpálčivejšie. Od samotného využívania AI systémov až po ich etické a právne aspekty, každé takéto stretnutie nám pomohlo získať nové perspektívy, odpovede a často aj ďalšie otázky.

Na základe diskusií sme sa rozhodli zosumarizovať päť najčastejších otázok a relevantných odpovedí. Vzhľadom na extrémne rýchly vývoj akejkoľvek oblasti týkajúcej sa AI majú však len obmedzenú trvanlivosť, ale môžu vám poslúžiť ako zdroj do diskusie, ktorú by ste vo firme mali mať – s manažérmi, so zamestnancami, s vývojármi, so správcami IT, s bezpečnostnými špecialistami a kýmkoľvek, kto sa u vás zaujíma o AI a jej implementáciu v reálnom svete.

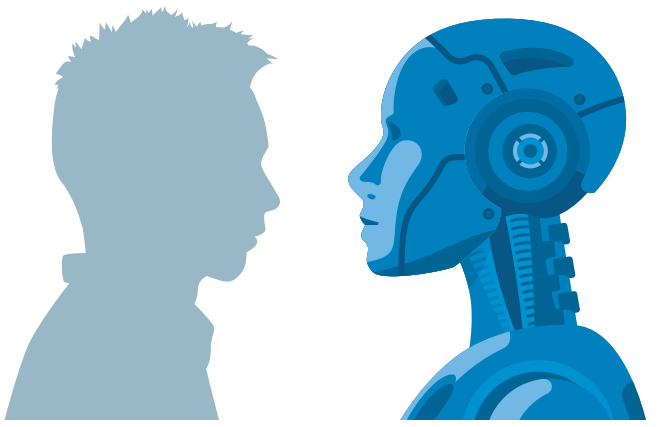
Či už hľadáte spôsoby, ako optimalizovať podnikové procesy, alebo chcete pochopiť riziká spojené s používaním verejne dostupných AI nástrojov, dúfame, že vám táto strana bude inšpiráciou.

Martin Lohnert,
riaditeľ centra kybernetickej bezpečnosti void SOC od Soitronu
Andrej Jenčo,
manažér oddelenia Data Intelligence, Millennium

Zničí AI ľudstvo? Alebo našu firmu? Prídem kvôli AI o prácu?

Nikto nedokáže s istotou predpovedať budúcnosť, a preto je dôležité uvažovať o rôznych možných scenároch. Záleží na vás, či sa v kontexte technológií prikloníte skôr k zástancom smeru „solarpunk", zameranému na optimistickú budúcnosť, kde ľudia žijú v harmónii s prírodou pomocou moderných technológií vrátane AI, alebo ak aj veríte viac v dystopické kyberpunkové scenáre a ste zástancom „lunarpunku", kde ľudia budú zrejme prežívať v drsných podmienkach, aspoň máte dostatok času sa naň pripraviť.

Oveľa menej času však máme na príchod AI v pracovnom, firemnom prostredí. Ak sa na ohrozenie AI pozeráme z pohľadu firmy, nebude to samotná umelá inteligencia, kto vašim zamestnancom vezme prácu. Bude to skôr nejaký iný človek, konkurent, kto dokáže nástroje AI využiť skôr a lepšie ako vy. A preto firmy, ktoré úspešne integrujú AI do svojich procesov a naučia svojich zamestnancov efektívne ju využívať, získajú významnú konkurenčnú výhodu. A zároveň nás všetkých pomôžu posunúť k svetlým „solarpunk" zajtrajškom.



Aké riziká mi hrozia pri používaní bežne dostupných AI nástrojov?

Používanie verejne dostupných AI nástrojov prináša viacero rizík, ktoré by ste mali dôkladne zvážiť.

- **únik citlivých informácií** – používanie AI v podnikovom prostredí môže viesť k neúmyselnému zdieľaniu dôverných údajov s treťou stranou,
- **„halucinácie"** – AI nástroje často poskytujú vierohodné, no nesprávne a vymyslené informácie,
- **nepresné výsledky** – AI nástroje môžu byť „naučené" na nekvalitných dátach, čo vedie k nepresným výstupom,
- **autorské práva** – vznikajú otázky o použití dát chránených autorskými právami pri trénovaní AI, alebo o vlastníctve AI výstupov

Ako využiť bežne dostupné AI nástroje aj napriek ich rizikám vo svojom podnikaní?

Kľúčom je definovať základné firemné pravidlá, ako môžu (a majú) zamestnanci používať AI pri plnení pracovných úloh.

- **V kategórii „bez obmedzení"** by sa mali nachádzať prípady použitia, ktoré nepredstavujú riziko pre bezpečnosť alebo súkromie, a môžu byť voľne využívané všetkými zamestnancami. Napríklad generovanie marketingových textov, obrázkov či názvov prezentácií. Sem patria aj interne nasadené AI nástroje, ktoré rešpektujú platnú legislatívu i firemné politiky.
- Druhá kategória by mala zahŕňať scenáre, ktoré si **vyžadujú vyššiu opatrnosť**. Tu by mal výstup z AI nástroja pred jeho použitím posúdiť odborník. Typicky ide o písanie počítačového kódu či odborné analýzy všemožných kategórií.
- V „zakázanej" kategórii by v princípe mali byť všetky ostatné prípady, ale najmä tie, ktorých vstupy obsahujú akékoľvek citlivé alebo osobné údaje. Zamestnanci by určite nemali používať verejné AI nástroje na analýzu zmlúv, životopisov, vašich zdrojových kódov a podobne.

Ako nám s rizikami pomôže AI legislatíva?

Známy „AI Act" je právny rámec Európskej únie, ktorý má za cieľ regulovať využívanie umelej inteligencie s dôrazom na ochranu základných práv, bezpečnosť a transparentnosť. Netýka sa jednotlivcov, ale zameriava sa na firmy a inštitúcie, ktoré AI nástroje vytvárajú alebo používajú. AI systémy klasifikuje podľa rizík – od minimálnych po neprijateľné, a stanovuje požiadavky pre vysokorizikové aplikácie, ako sú tie v oblasti zdravotníctva, dopravy alebo vzdelávania. Cieľom je zabezpečiť, aby AI technológie boli využívané eticky a bezpečne, a aby mali používatelia a spoločnosť istotu, že nebudú zneužité.

V súvislosti s kyberbezpečnosťou – bude AI viac pomocou alebo príťažou?

AI je a bude zároveň významnou pomocou aj hrozbou. Už dnes sa strojové učenie využíva na detekciu hrozieb, vyhodnocovanie abnormálneho správania, filtrovanie škodlivého obsahu či triedenie veľkých objemov dát. Generatívna AI zase pomáha zvyšovať produktivitu technických špecialistov, poskytuje používateľom lepší prístup k báze znalostí alebo automatizuje mnohé (aj) bezpečnostné procesy.

Na druhej, temnej strane, AI môže rovnako pomáhať aj pri programovaní škodlivého kódu a sprístupňuje znalosti útočníkom. Očakávame, že v blízkej budúcnosti sa začneme stretávať s „automatizovanými" útokmi, kde sa škodlivé technológie budú učiť a prispôsobovať samy v reálnom čase.

Potrebuje ich celý svet

REPORTÁŽ

CyberGame predstavuje atraktívny a netradičný spôsob, ako nadchnúť profesionálov pre kybernetickú bezpečnosť.

Tri silné piliere CyberGame: za autorský tím Lukáš Balážik z Národného bezpečnostného úradu, absolútny víťaz tretieho ročníka Vojtech Bardiovský, zástupca hlavného partnera, Pavol Závacký, technický riaditeľ spoločnosti Alanata. FOTO: PRODUKCIA, S. R. O.

Na Slovensku akútne chýba desaťtisíc profesionálov kybernetickej bezpečnosti. Potrebujeme manažérov, právnikov, učiteľov, technológov, programátorov, analytikov aj architektov.

Hľadá ich celý svet. Naša národná kyberbezpečnostná súťaž oslovila vyše osemsto talentov.

Viac ako hra

V treťom ročníku národnej kyberbezpečnostnej súťaže CyberGame sa registrovalo vyše 2 300 účastníkov. Vo finále bodovalo 874 hráčov a hráčok, počínajúc prvákmi na strednej škole a končiac skúsenými programátormi.

Súťaž sa stáva komunitným fenoménom. Funguje aj ako fakultná liga, prípadne vybrané úlohy riešia stredoškoláci a pre profesionálov je CyberGame prestížna tréningová platforma, kde si môžu porovnať zručnosti.

Talenty to nevzdávajú

Základným poslaním CyberGame však zostáva hľadanie talentov, a to sa podarilo aj v prípade víťaza. Vojtech Bardiovský je programátor už viac ako desať rokov a jeho práca nesúvisí s kybernetickou bezpečnosťou. „O tému som sa začal zaujímať, keď som objavil pred dvomi rokmi CyberGame. Hra ma mimoriadne bavila, ale nemal som ani zďaleka vedomosti na umiestnenie, tak som začal vyhľadávať online úlohy. Baví ma zisťovať, ako veci fungujú, a popri tom si zasúťažiť."

Nadpolovičná väčšina hráčov CyberGame uviedla vek do 25 rokov. Víťaz študentskej kategórie bude viesť kyberbezpečnostný reprezentačný Team Slovakia na európskom finále European Cyber Security Challenge.

Potrebujete ľudí aj nápady

„Vymyslieť a naprogramovať kyberbezpečnostnú hru je extrémne náročné. Sú na to nevyhnutné nielen skúsenosti a odborné vedomosti, ale aj kreativita, ako otázky a úlohy vysvetliť a sformulovať," hovorí Jaroslav Ďurovka, riaditeľ Národného centra kybernetickej bezpečnosti.

CyberGame 2024 sa už druhý rok hrala na slovenskej aj anglickej platforme a účastníci boli okrem Slovenska z viac ako päťdesiatich štátov.

Na obsahu záleží

Úlohy pripravili profesionáli z praxe, keďže odborným garantom súťaže je Národný bezpečnostný úrad. V treťom ročníku CyberGame sa „hrali" tri analytické vetvy – malvérová, forenzná a OSINT analýza, ďalšie vetvy boli venované kryptografii a procesom a riadeniu bezpečnosti. Účastníkov pritiahla aj novinka, ofenzívna bezpečnosť.

Zatiaľ čo prvý rok dosiahol plný počet bodov iba víťaz, v treťom ročníku to bolo sedem hráčov. „Príjemne nás prekvapil väčší počet úspešných riešiteľov, čo svedčí o rastúcej úrovni súťažiacich. Taktiež sme získali viac spätnej väzby, čo nám pomôže ešte viac zlepšiť CyberGame v budúcnosti," hodnotí aktuálny ročník Lukáš Balážik, člen autorského tímu.

Ocenenie bolo udelené v rôznych kategóriách s prihliadnutím na vek aj odbornosť. Najlepšie hrajúci učiteľ je Peter Švec z Fakulty prírodných vied a informatiky UKF v Nitre. Zapojil sa rovnako ako v minulom roku s motiváciou naučiť sa o rôznych hrozbách a nových postupoch riešenia problémov kybernetickej bezpečnosti.

> VYMYSLIEŤ A NAPROGRAMOVAŤ KYBER-BEZPEČNOSTNÚ HRU JE EXTRÉMNE NÁROČNÉ.
>
> **Jaroslav Ďurovka,** riaditeľ Národného centra kybernetickej bezpečnosti

K tejto skúsenosti sa pripája aj Michal Šrobár, učiteľ kyberbezpečnosti na 1. Súkromnom Banskobystrickom gymnáziu. Jeho hráčsky výkon ho nominoval na experta v analýze otvorených zdrojov OSINT.

Peter Švec pridáva aj aktualizáciu: „Pri riešení úloh mi veľmi pomohol jazykový model umelej inteligencie, ktorý zrýchľuje a zjednodušuje niektoré činnosti. Osobne som ho využíval pri prepisovaní kódu z jedného jazyka do iného a hľadaní súvislostí, ktoré na prvý pohľad nie sú zrejmé. Musím povedať, že oproti minulému roku sa AI zlepšila a už je pri riešení úloh nápomocná, avšak stále treba rozmýšľať nad tým, čo vygeneruje, a to je dobré."

Talenty to nevzdávajú

Expert vo vetve kryptografia zverejnil iba krstné meno a je zamestnaný ako implementátor automatickej logistiky. Rieši nielen integráciu softvéru na serveroch zákazníka, ale aj programovanie logiky, ako riadiť tok materiálu prevážaného autonómnymi vozíkmi.

Maroš hodnotí CyberGame ako veľmi poučnú, aj keď neraz našiel „scenár, kde som natrafil na akýsi pomyselný múr, ktorý som nakoniec kúsok po kúsku zbúral. Tento ročník hodnotím ako najlepší z hľadiska úloh. Boli interaktívnejšie, zábavnejšie, ale aj najviac naučili. Vďaka cybergame som si precvičil a vycibril svoje programátorske skúsenosti, za čo patrí organizátorskému tímu veľká vďaka."

PORADŇA

Zoberte si na pomoc aj virtuálneho asistenta

Firmy čelia mnohým kybernetickým hrozbám, ktoré ich môžu zasiahnuť cez široké spektrum vektorov. Správcovia zodpovední za IT bezpečnosť tak majú neľahkú úlohu reagovať na detekcie z rôznych bodov – od počítačov cez mobilné zariadenia až po cloud.

Orientovať sa v množstve hlásení, z ktorých niektoré môžu byť len falošnými poplachmi, je mimoriadne náročné. Stáva sa, že aj skúsení analytici sú natoľko preťažení, že ich vnímanie hrozieb je zahmlené pribúdajúcim množstvom úloh. Umelá inteligencia však umožňuje tieto výzvy riešiť.

Bezpečnosť na pár kliknutí

Špičkové bezpečnostné technológie ako rozšírená detekcia a reakcia (XDR) si vyžadujú na svoju správu značné množstvo vysokokvalifikovaných pracovníkov. Firmy preto riešia túto situáciu automatizáciou pomocou technológií založených na umelej inteligencii alebo outsourcingom služieb kyberbezpečnosti.

Umelá inteligencia už významne pomáha administrátorom v rámci XDR riešenia ESET Inspect s koreláciou a kontextualizáciou detekcií. Vďaka tomu môžu začínajúci aj pokročilí správcovia lepšie porozumieť detekciám, čo vedie k rýchlejšej a presnejšej reakcii. Funkcia automatizovaného vytvárania incidentov odbremeňuje bezpečnostných pracovníkov od zdĺhavého zaznamenávania incidentov, čo im umožňuje venovať sa strategickej agende.

Bezpečnostným administrátorom prácu ešte viac uľahčí virtuálny asistent. ESET AI Advisor pomôže operátorom identifikovať, analyzovať a zmierniť hrozby prostredníctvom konverzačných podnetov a interaktívneho dialógu, čím sa plnenie bezpečnostných úloh zredukuje na niekoľko kliknutí.

Spoľahlivý asistent

ESET AI Advisor je generatívny asistent kybernetickej bezpečnosti založený na umelej inteligencii, ktorý ponúka personalizované poznatky a okamžitú pomoc prispôsobenú špecifickým potrebám organizácie. Bezpečnostným analytikom pomáha s jednou z najčastejšie sa opakujúcich úloh – s vyšetrovaním incidentov.

Chatbot poskytuje relevantné a praktické poznatky v reálnom čase. Zjednodušuje komplexné informácie o hrozbách a sprístupňuje ich aj menej skúseným odborníkom v oblasti IT bezpečnosti. Umožňuje tak bezpečnostným analytikom s rôznymi úrovňami zručností rýchlo reagovať na kritické situácie a minimalizuje následky narušenia bezpečnosti, čo vedie k efektívnejšej správe incidentov.

Tento trendový nástroj navyše dokáže automatizovať zdĺhavé úlohy, ako je zber dát, extrakcia a základné vyhľadávanie či detekcia hrozieb. Dokáže tiež označiť neobvyklé alebo podozrivé správanie a pomáha bezpečnostným tímom prijať príslušné opatrenia. Taktiež asistuje pri rozpoznávaní pokusov o phishing a radí používateľom, ako sa nestať obeťou podvodných e-mailov alebo webových stránok. Nástroj ESET AI Advisor je aktuálne v ponuke ako súčasť XDR modulu ESET Inspect v rámci úrovne ochrany ESET PROTECT MDR Ultimate.

Igor Kmiť,
PR Specialist ESET Slovensko

Bezpečnostné technológie na báze umelej inteligencie sú už štandardom. FOTO: DREAMSTIME

RIEŠENIE

Prediktívna bezpečnosť a umelá inteligencia. Výborne si rozumejú

Prediktívna bezpečnosť je zásadný pilier kyberbezpečnosti. Využíva pokročilé analytické nástroje a technológie na predikciu a prevenciu hrozieb. Chce vedieť o útokoch skôr, než nastanú. Bez diskusie – najefektívnejšie riešenie.

Lákavé terče

Zdravotníctvo je pre útočníkov lákavým terčom najmä pre kombináciu cenných osobných dát, často zastaraných systémov a nízkych rozpočtov na ochranu. Úspešný útok by mohol byť likvidačný. Preto sa jeden z našich zákazníkov po náraste počtu incidentov obrátil na nás so žiadosťou o pomoc.

Zdravotnícka spoločnosť potrebovala ochrániť svoju sieť, ktorá zahŕňa viac než desať nemocníc, kancelárie v 120 lokalitách a desaťtisíce zamestnancov v USA.

„Ponúkli nám plne integrované riešenie, ktoré dokonalo prepojili s našimi starými bezpečnostnými systémami. Pokrýva každú fázu detekcie a prevencie hrozieb. Vzhľadom na naše povinnosti vyplývajúce z regulácie zlepšili aj celkové reakčné schopnosti," zhodnotil výsledok riaditeľ pre informačnú bezpečnosť zdravotníckeho holdingu.

Útoky tu budú stále

Vybrali sme službu AIsaac, lebo je ideálna pre organizácie, ktoré už majú zavedený bezpečnostný monitoring a implementované rôzne nástroje. Rozsah úloh a nedostatok ľudských kapacít im však bránia posunúť sa na vyššiu úroveň, ktorú si vyžaduje implementácia umelej inteligencie na „temnej" strane. Služba je vhodná aj pri presune do cloudu či zabezpečení hybridných prostredí. Využitie má práve v regulovaných odvetviach, ktoré majú vysoké nároky na ochranu dát a zároveň patria medzi najčastejšie terče kybernetických útokov.

Reakcia na kybernetický útok je zložitý proces, ktorý si okrem najnovších znalostí vyžaduje presnú koordináciu a postupy. Reakcia musí pokryť on-premise, hybridné, aj multicloudové prostredie organizácie, aby nikde nezostali slepé miesta. Umelá inteligencia celý tento proces zrýchľuje.

Ochrana krok za krokom

Platforma AIsaac integruje bezpečnostné nástroje zákazníka a zdroje údajov z internetu do jedného rámca. To umožňuje ochrániť všetky digitálne aktíva pomocou jedinej platformy naprieč všetkými vrstvami zabezpečenia.

Prvým krokom je Threat Intelligence, čiže nepretržité monitorovanie informačných kanálov a prehľadávanie prostredia globálnych hrozieb. Viac ako sto nasadených bezpečnostných analytických modelov so strojovým učením zároveň vyhodnocuje globálne hrozby a dokáže sa zamerať aj na špecifické riziká pre geografický región či odvetvie.

Služba zároveň analyzuje potenciálne slabé miesta v organizácii vrátane sietí, používateľov, aplikácií a koncových bodov a vzorcov správania. Darí sa tak reagovať aj na pokročilé hrozby, ktoré by inak zostali neodhalené. V závislosti od implementácie dokáže automaticky spúšťať mitigačné opatrenia a obnovu zasiahnutých systémov a dát.

Veľmi dôležitý aspekt

Prediktívny charakter služby umožňuje bezpečnostným tímom pripraviť sa na hrozby ešte skôr, ako nastanú. Ako sa vraví, najlepší je ten kybernetický incident, ktorému sa dokážeme vyhnúť.

Platforma AIsaac využíva generatívnu umelú inteligenciu a veľké jazykové modely. Sú postavené na súhrne všetkých poznatkov a skúseností spoločnosti Eviden súčasne s hrozbami a reakciami na ne. Po potenciálnych hrozbách naši experti pátrajú aj v temných zákutiach internetu – na darknete, následne ich vyhodnocujú a vypracujú odporúčania. Službu dopĺňame o informácie a analýzy, ktoré nie sú dostupné z verejných zdrojov.

Primárnym účelom služby je automatizovať detegovanie incidentov a spúšťanie reakčných procesov. Výsledkom je rýchla analýza potenciálnych útokov a vyhodnotenie ich možného dosahu. Riešenie obsahuje informácie o pôvode hrozby a bráni šíreniu útoku. Bezpečnostný tím tak má k dispozícii presné a vykonateľné odporúčania a návrhy ďalších krokov.

Zlepšenie od prvého dňa

Vráťme sa však k sieti zdravotníckych zariadení. Bezpečnostná situácia sa zlepšila už v prvý deň. Integrácia AI platformy do existujúcej bezpečnostnej infraštruktúry znížila objem falošne pozitívnych výsledkov o viac ako 75 percent a priemerný čas detekcie o viac ako 80 percent.

Spoločnosť dosiahla a dokázala udržiavať takmer dokonalý súlad s bezpečnostnými požiadavkami. Darilo sa aj identifikovať potenciálne hrozby a reagovať na ne takmer v reálnom čase.

Michal Sekula,
bezpečnostný konzultant
Eviden Slovakia