HN
obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

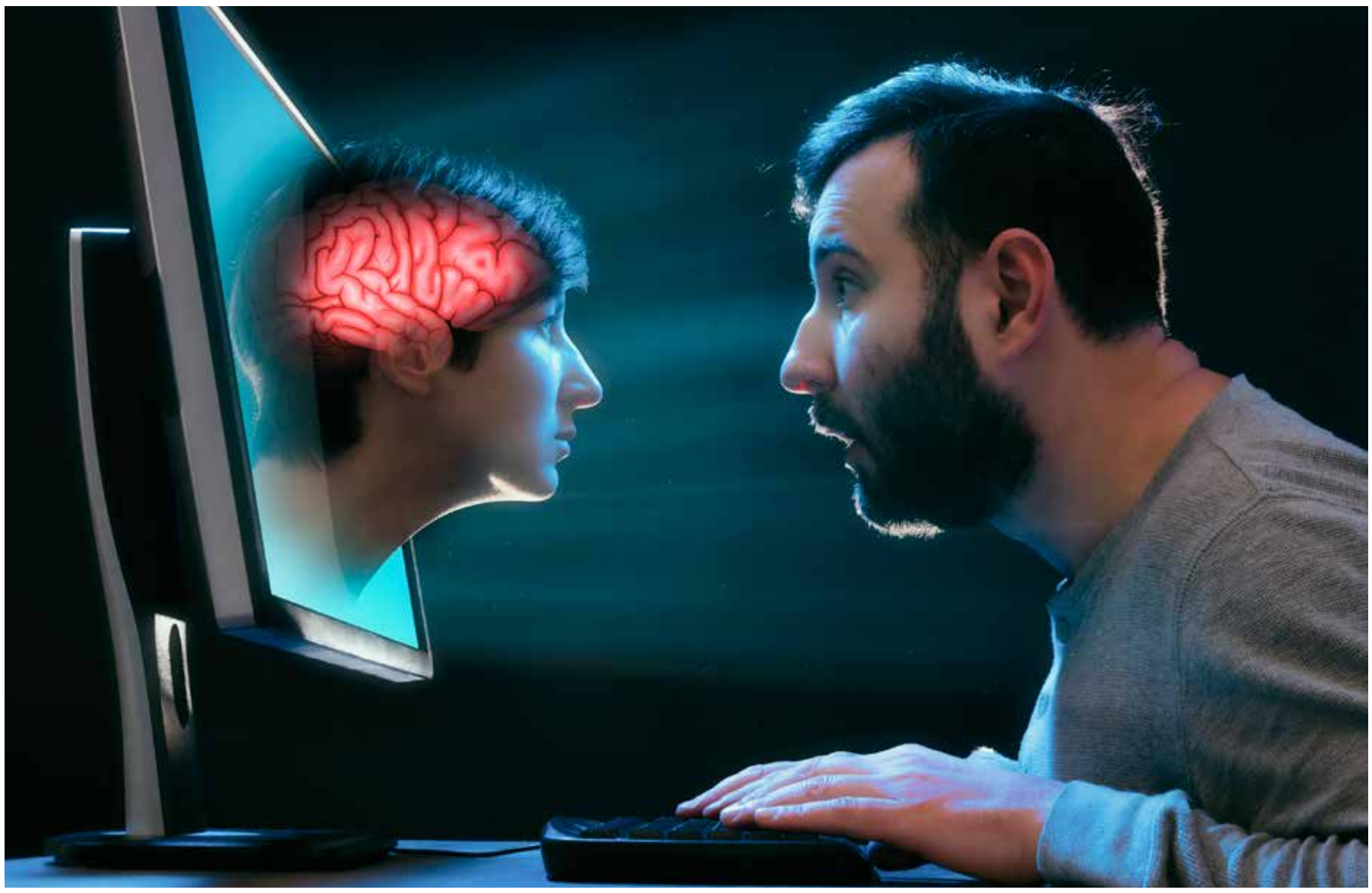
PIATOK – NEDEĽA
28. – 30. JÚLA 2023

Partneri špeciálnej prílohy:
ALISON
ALITER TECHNOLOGIES

Útok, obrana, vylepšenie a zas znova

TÉMA

Uplatnenie umelej inteligencie aj bezpečnostní profesionáli prirovnávajú k Pandorinej skrinke, ktorá sa už nedá zavrieť, alebo ku kambrickej zmene, ktorá navždy zmení svet. Pardon, už ho zmenila.



Budeme potrebovať ľudí, ktorí budú schopní používať aplikácie umelej inteligencie, komunikovať s nimi a koexistovať s týmto fenoménom. SNÍMKA: DREAMSTIME

Vy ešte nemáte bot?

Vo Východoslovenskej energetike si kúpili phishingového bota.

Funguje s pomocou umelej inteligencie a pomáha trénovať zamestnancov. Phishingové útoky sa valia na používateľov každý deň a rovnako ako všetko, aj odolnosť proti nim treba trénovať.

„Princíp je v tom, že bot sleduje trendy vo svete phishingových mailov a vytvára vlastné kampane tak, aby boli čo najviac autentické a na nerozpoznanie od legitímnych mailov," približuje fungovanie Lukáš Gábor, špecialista na kyberbezpečnosť.

Nástroj sa učí sám. Ak bot zistí, že nejaký typ mailov zamestnanec ignoruje, bude mu posielať iné typy a zisťovať, kde ho nachytať. Presne tak, ako to robia útočníci a ich phishingové boty.

Sladké vábenie AI

Počas kampane sa snaží bot zamestnancov nahovoriť na to, aby klikali na odkazy v tele mailu alebo v prílohe. „Maily vyzerajú veľmi dobre a stačí trocha nepozornosti a kliknete bez zaváhania," opisuje Lukáš Gábor.

Ak niekto klikne, neublíži mu to. Systém ho upozorní a ponúkne výučbový materiál na doplnenie vedomostí. Kampaň sa vyhodnocuje a graficky zobrazuje štatistiky a trendy.

A financie? Energetici považujú phishing bot za „veľmi dobrú investíciu". Počet preklikov im za pol roka klesol z 26 percent na 10,6. Pre bezpečákov aj pre zákazníkov je to vynikajúca správa – kyberodolnosť energetiky sa zvyšuje.

Zvažujme riziká

Či už ide o finančný sektor, medicínu, ozbrojené zložky alebo výrobu, musíme byť obozretní pri uplatnení umelej inteligencie. Tibor Szabo pracuje v oblasti auditu bezpečnosti a IT takmer tri desiatky rokov, z toho osem rokov vo VÚB, a preto okrem nadšenia upozorňuje aj na ohrozenia.

Medzi nástrahy zaraďuje nesprávne sformulovanú otázku v konverzačných aplikáciách, nedostatočnú ochranu citlivých údajov, nedodržanie etických pravidiel pri vývoji a prevádzkovaní AI či neoverenú interpretáciu výstupov s dosahom na klientov.

„Klienti, a to nielen v bankovom sektore, budú musieť byť informovaní, že prichádzajú do styku s umelou inteligenciou," prízvukuje Tibor Szabo. Táto klauzula im umožní rozhodnúť sa, či službu využijú.

Katastrofický scenár

Razantný a široký nástup systémov umelej inteligencie otvára aj tému, ako odolajú kyberhrozbám. Útočník sa tu môže pokúsiť o zmenu použitia alebo ohrozenie bezpečnostných vlastností systémov. Typickým príkladom útoku a zneužitia systému je takzvaný data poisoning alebo „otrávenie údajov".

Ide o kyberútok na súbory trénovacích údajov a manipuláciu s týmito súbormi. Útočník vkladá „otrávené" údaje do súborov, aby mohol kontrolovať správanie trénovaného modelu a poskytovať falošné výsledky. Napríklad označí spam alebo infikovaný e-mail ako bezpečný e-mail.

Čo na to obrancovia

Kyberbezpečnostní profesionáli si dávajú ďalšie úlohy. „Hľadáme a vylepšujeme spôsoby využitia umelej inteligencie a strojového učenia v obrane a študujeme, ako ich používajú útočníci," vysvetľuje Milan Pikula z Národného centra kybernetickej bezpečnosti SK-CERT. Na ďalšej úrovni sa zaoberajú dosahmi zaujatosti pri tréningu modelov a ich využití. S rastúcou popularitou jazykových modelov rastie aj ich využitie útočníkmi. Výsledkom sú dôveryhodnejšie phishingové kampane, viac cielených útokov metódou sociálneho inžinierstva, aj jednoduchšia produkcia falošných správ a dezinformácií. Preto zástupcovia autorít akcentujú aj akútnu potrebu šírenia povedomia.

Už sa to nedá vrátiť

Jazykové modely uľahčujú aj bezpečákom rešerše, jazykové korektúry, preklady, analýzy hlásení o zraniteľnostiach, analýzu malvéru, návrh textov či vývoj nástrojov aj rozsiahlejšieho softvéru.

„Ak potrebujem rýchlo vytvoriť prototyp aplikácie alebo spojiť existujúce nástroje na vyriešenie akútneho problému, namiesto písania vlastného kódu poprosím GPT model, aby kód vygeneroval za mňa," opisuje uplatnenie v praxi Ján Skalný z SK-CERT. Pochopiteľne, je potrebné vedieť, čo objednávateľ od AI programátora chce, a potom sa objednávateľ už ako programátor s modelom vyladí.

Zhoda na tom, že umelá inteligencia ako nástroj je už príliš silná, panuje naprieč sektormi. Zároveň už niekoľko rokov je aj veľmi významnou témou rozvojových programov financovaných z grantov EÚ. „Táto trhlica sa už nedá zavrieť," glosuje Milan Pikula.

Prvá právna regulácia AI

Navrhovaný európsky Akt o umelej inteligencii zdôrazňuje kľúčovú úlohu kyberbezpečnosti pri zabezpečovaní odolnosti systémov. Akt stanovuje, že zásady bezpečnosti pre systémy AI budú navrhnuté a vyvinuté už v štádiu koncepcie. Bezpečnostné riešenia a záplaty sa budú vyžadovať počas celého životného cyklu systému.

Predpokladá sa, že Akt o umelej inteligencii bude prijatý do konca roka 2023 a vykonávať sa začne o tri roky neskôr. Má povahu nariadenia, a preto sa nevyžaduje jeho transpozícia do právnych poriadkov členských štátov. „Dôveryhodnosť systémov umelej inteligencie nemôže existovať bez vysokej miery kyberodolnosti," prízvukuje Miroslav Chlipala, riadiaci partner BCH Advokáti Chlipala.

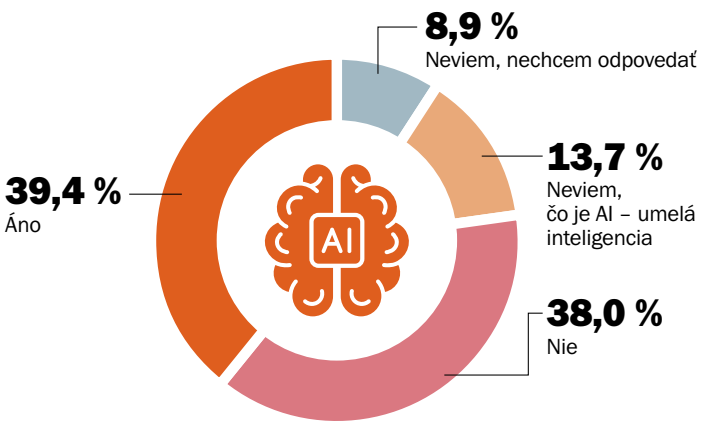
Čaká nás diskusia

V dlhodobom horizonte odborníci upozorňujú na riziko technologickej singularity, keď sa rast schopností AI vymkne nášmu pochopeniu a kontrole. Navrhovaný akt preto budí pozornosť celého sveta, akademikov aj skúsených profesionálov.

Ján Skalný z SK-CERT preto upozorňuje aj na riziko, ktoré predstavuje striktná regulácia výskumu a aplikácie umelej inteligencie v kontexte hybridných hrozieb, ktorým Európa čelí.

Prehnaná regulácia môže zbrzdiť inováciu v rôznych odvetviach a poškodiť európsku konkurencieschopnosť. Zároveň nerovnováha v regulácii, spolu s nevynútiteľnosťou globálnych pravidiel, umožní nedemokratickým krajinám využívať AI na šírenie dezinformácií a škodlivého obsahu bez akýchkoľvek obmedzení. A to vrátane dnes ešte neznámych spôsobov využitia.

Máte alebo nemáte obavy z AI – umelej inteligencie?



Zdroj: Reprezentatívny online prieskum Kybernetická bezpečnosť 2023, verejnosť SR. Realizácia agentúra AKO pre KCCKB

NAJČASTEJŠIE MÝTY V SÚVISLOSTI S UMELOU INTELIGENCIOU

Jazykový model rozmýšľa a má vlastný názor.
Aplikácia je niečo ako priateľ na telefóne, čo si stihol prečítať viac dokumentácie.

Umelo natrénované obmedzenia znemožnia útočníkom používať model so zlým úmyslom.
Zatiaľ ich vždy bolo možné hravo obísť.

Umelá inteligencia dnes nahradí ľudských odborníkov.
Aplikácia v podobe jazykových modelov významne neohrozí žiadnu oblasť.

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti · auditori.it · CHECK POINT · ESET · Progress · SOITRON · SK CERT NÁRODNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 28. – 30. JÚLA 2023

Čo robiť, keď sa už minú argumenty

ANKETA

Na čo nám je investícia do kyberbezpečnosti? Už stokrát počuli túto otázku. Argumentovali predstavenstvu, finančným riaditeľom, vedeniu organizácií, zákazníkom aj zákonodarcom. Vtedy bezpečnostní profesionáli upúšťajú od formálnej strohosti, nadýchnu sa a ponúknu poslednú možnosť.

Rastislav Janota,
riaditeľ
Národné centrum kybernetickej bezpečnosti SK-CERT

V každom rozhovore sú dve strany. Jedna žiada o investície, respektíve iné vstupy, a argumentuje a druhá počúva a rozhoduje. V živote sa však stretávame často aj so situáciou, kde poslucháč nie je ochotný počúvať ani veľmi silné a dobré argumenty, alebo proste nie je schopný im porozumieť – nemá na to dostatočné vedomosti. A vtedy často pomôže, až keď sa čierne predpovede splnia a škoda nastane. Ale to je už veľmi neskoro.

Roman Čupka,
hlavný konzultant
Progress a CEO Synapsa Networks

Argumentovať by sa malo na základe toho, s kým sa bavíte. A tak aby sa zobrali do úvahy všetky skutočnosti, ktoré druhá strana v danej chvíli považuje za najaktuálnejšie. Pokiaľ však niekomu argumenty nepostačujú, odporučím riadiť sa príslovím, že aj najtuhšie drevo raz prehorí. Záleží potom na veľkosti požiaru, ktorý ten oheň spôsobí.

Ján Grujbár,
generálny riaditeľ
Aliter Technologies

Povedzme si skôr, čím treba začať. Informačná bezpečnosť je často vnímaná ako akýsi protivietor biznisu a toto nastavenie je potrebné otočiť. Investície do informačnej bezpečnosti musia byť jednoznačne zladené s firemnými cieľmi – vychádzať z nich a ideálne ich dokonca podporovať. A ak to nestačí, treba vyložiť na stôl všetky možné riziká aj s dôsledkami, v plnej miere ich kvantifikovať a toto je bod, keď dochádza k uvedomeniu.

Andrej Žucha,
generálny riaditeľ
ALISON Slovakia

Ak nefungujú racionálne argumenty, tak zostáva už len čakať na prvý incident. Vtedy si organizácie začnú uvedomovať, o čo všetko prišli a akú tú má pre nich vysokú hodnotu.

Ivan Makatura,
generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Pokiaľ zvažujete, či vám ako „bezpečnostné opatrenie“ bude stačiť dokumentácia, vedzte, že papierová bezpečnosť má dve nesporné výhody: 1. Je lacná. 2. Vydrží až do likvidácie firmy, ktorá nastane po závažnom incidente. Ďakujem, že ste ma vypočuli.

Tomáš Hettych,
viceprezident
ISACA

V tomto momente presne prichádza čas na „teologickú“ bezpečnosť. Všetci musia začať veriť, že sa organizácii nemôže nič stať. K tomu im len zaželám veľa šťastia, aby ich obišli všetky kyberbezpečnostné hrozby a incidenty.

Ján Andraško,
SOC Manažér
Binary Confidence

Anonymizované príklady z početného množstva riešených bezpečnostných incidentov vo firmách, ktoré bezpečnosť „tiež nepotrebovali“. To ešte stále dokáže pomôcť zmeniť názor zodpovedných.

Ivan Kopáčik,
bezpečnostný expert
Gordias

Vždy sa nájde aktuálne medializovaný bezpečnostný incident väčšieho rozsahu. „Zajtra takto môžu písať o vás, zoberiete na seba to riziko a jeho dôsledky?“ je argument, ktorý zvyčajne otvorí vecnú diskusiu o potrebách investícií do kyberbezpečnosti.

Július Selecký,
senior technický špecialista
ESET

Treba to zobrať ako ochranu online života. Rovnako ako zamkýname dvere, nastavujeme alarm a možno používame aj kamery. Kybernetická bezpečnosť je to isté len v digitálnom svete. V konečnom dôsledku, ak sa niečo stane a ja som neinvestoval do týchto virtuálnych zámkov, vyzerám v dnešnej dobe tak, ako keby som zaspal v tých zámkoch zo stredoveku.

Tomáš Valenta,
riaditeľ
Check Point Software Technologies na Slovensku

Poistiť si život, auto či dom je pre väčšinu pochopiteľné na prvú dobrú. Zabezpečiť svoju firmu, a teda svoj príjem, by nemalo byť o nič zložitejšie. Takmer každý vie vyčísliť riziká v prípade kyberútokov, len sa musí zamyslieť. Nie vždy ide „len“ o peniaze. Asi najhorším scenárom je výpadok v nemocniciach, odklad operácií pacientov, a tým ohrozenie životov. A to nechce nikto. Môže ísť o nás alebo našich blízkych.

Diana Legdanová,
vedúca úseku bezpečnosti
Východoslovenská energetika Holding

Popravde, nestála som ešte pred takou otázkou. Náš topmanažment počúva na racionálne argumenty, čo nám dovoľuje energiu venovať do samotnej realizácie. Ale keby som takúto otázku dostala, odpovedala by som protiotázkou: Prečo si doma chránite rodinné šperky, rodné listy alebo aj niektoré fotky v mobile? Alebo – koľko ste ochotní zaplatiť hackerovi za to, aby nezverejnil všetky dáta o vašich zákazníkoch?

Jaroslav Oster,
predseda správnej rady
Preventista.sk

Z praxe dva argumenty odskúšané ako fungujúce. V prvom rade je to osobná zodpovednosť štatutára vrátane trestnoprávnej zodpovednosti, rovnako aj trestná zodpovednosť organizácie. Druhým je zvyšovanie odolnosti organizácie proti zneužitiu infraštruktúry, a teda predchádzanie situácii, keď sa infraštruktúra organizácie môže stať nástrojom páchania rôznych foriem trestnej činnosti.

Jakub Berthoty,
advokát
Dagital Legal

Väčšinou keď už príde právnik na ochranu osobných údajov do firmy, ktorá neinvestovala do kybernetickej bezpečnosti, tak už o tom nikoho presviedčať nemusí.

Ján Adamovský,
riaditeľ bezpečnosti
Slovenská sporiteľňa

Kybernetická bezpečnosť je komplikovaná téma, preto je dôležité ju komunikovať v reči, ktorej publikum rozumie. Pokiaľ je napríklad kľúčový člen vedenia vášnivý pilot, odporúčam toto: Riadiť spoločnosť bez vyspelých technických nástrojov kyberbezpečnosti je ako pilotovať bez prístrojov. Pre malé lietadlá sa to dá, aj keď je to extrémne náročné. Pre veľké dopravné je to nemožné určite.

Martin Oczvirk,
riaditeľ odboru informačnej bezpečnosti a certifikácie
Úrad na ochranu osobných údajov

Reálne už môžem len rezignovane sucho skonštatovať – urobil som, čo sa dalo. Ale ešte mám posledný argument, možno alibistický. Ak nastane incident a firma bude v hľadáčiku príslušných bezpečnostných autorít, bezpečákovi „hlava na krku“ pravdepodobne ostane, keďže upozorňoval na hroziace riziká. Informovať manažment o riziku neinvestovania do kyberbezpečnosti a hroziacich pokutách patrí medzi naše povinnosti.

Martin Lohnert,
riaditeľ centra kybernetickej bezpečnosti Void SOC
Soitron

Bohužiaľ, aj s tým sa stretávame v praxi. Človek, ktorý v organizácii zodpovedá za kybernetickú bezpečnosť, prichádza s návrhmi zlepšenia, podloženými racionálnymi argumentmi. Napriek tomu sú návrhy zamietané, ale zodpovednosť ponechaná, čo skôr či neskôr vyústi do frustrácie a odchodu človeka. V horšom prípade aj do naplnenia rizík, ktoré návrhy adresovali. Zdá sa však, že pomaly pribúda manažérov aj mimo IT, ktorí v bezpečnosti na argumenty počúvajú a dokážu sa použiť na chybách iných.

Timea Tomčová,
manažérka informačnej bezpečnosti
Poisťovňa Union

Opatrenia implementované v oblasti kyberbezpečnosti majú byť primerané. Čo sa asi jednoduchšie konštatuje, ako pretaví do reality. Preto ak sa rozhodujete, kam dáva zmysel investovať ľudské, časové alebo finančné zdroje, je dobré riadiť sa takzvaným zdravým sedliackym rozumom a logikou. Tento prístup zriedkakedy sklame.

Richard Kiškováč,
generálny riaditeľ
Elkan

Do pozície, keď sa minú všetky formálne argumenty pre investície do kyberbezpečnosti, by sa skúsený manažér nemal nikdy dostať. Dostatočné množstvo argumentov musí poskytnúť dobre nastavený proces riadenia rizík. Treba mať pod kontrolou všetky významné zmeny, ako aj nové projekty a formálne vyhodnocovať riziká už v počiatočných fázach. V opačnom prípade sa investície do zmenšenia rizík značne predražia.

Tibor Paulen,
manažér informačnej bezpečnosti
Stredoslovenská distribučná

Predstavte si, že zdedíte dom, ktorý nemá vchodové dvere, okná sa nedajú zavrieť a v jeho pivnici je tmavý tunel, ktorý vedie nevedno kam. Presne k takémuto domu by sa dali prirovnať vaše IT systémy, ak by neboli zabezpečené. Nasťahovali by ste sa do takéhoto domu? Nechali by ste v ňom svoje cenné veci? Alebo by ste najskôr investovali do jeho bezpečnosti?

Marián Illovský,
audítor kybernetickej bezpečnosti
Auditori.it

Ak sa minú odborné argumenty, relevantné k téme, prechádzam na analógie zo života. Napríklad ako vysvetliť riziko súvisiace s „any to any“ pravidlom na firewalle. Ak má vrátnik vyložené nohy na stole a zdvihnutú rampu do areálu a ani sa nepozrie, kto vchádza, tak to asi nie je želaný stav. Ale ak zastaví každého, opýta sa, kam ide, a overí si to u príslušného vlastníka domu, tak to je to, čo od neho chceme. A zrazu si všetci vo vedení organizácie uvedomili riziká.

Henrich Šnajder,
manažér IT bezpečnosti
Orange Slovensko

Kybernetické útoky sú čoraz častejšie a sofistikovanejšie a môžu mať pre organizácie katastrofálne následky. Únik dát, výpadky systémov a ransomvérové útoky môžu poškodiť povesť, viesť k strate zákazníkov či narušiť chod štátu a stáť milióny eur. Investícia do kybernetickej bezpečnosti je preto nevyhnutná na ochranu pred týmito hrozbami.

Zuzana Motúzová,
advokátka
Motúzová & Lacko Advokátska kancelária

Argumenty, na čo nám je investícia do kybernetickej bezpečnosti, sa minúť nemôžu. Vždy bude existovať ďalší uhol pohľadu, pretože systémy našich klientov sa neustále rozvíjajú a hackeri nespia. A ak sa predsa len minú, zaberá príbeh o upratovačke. Upratovačka je predsa najväčší hacker, najmä ak nedodržiavame zásadu čistého stola. A to vždy zaberie.

Jozef Zoričák,
vedúci oddelenia informatiky
Národný ústav pľúcnych chorôb Vyšné Hágy

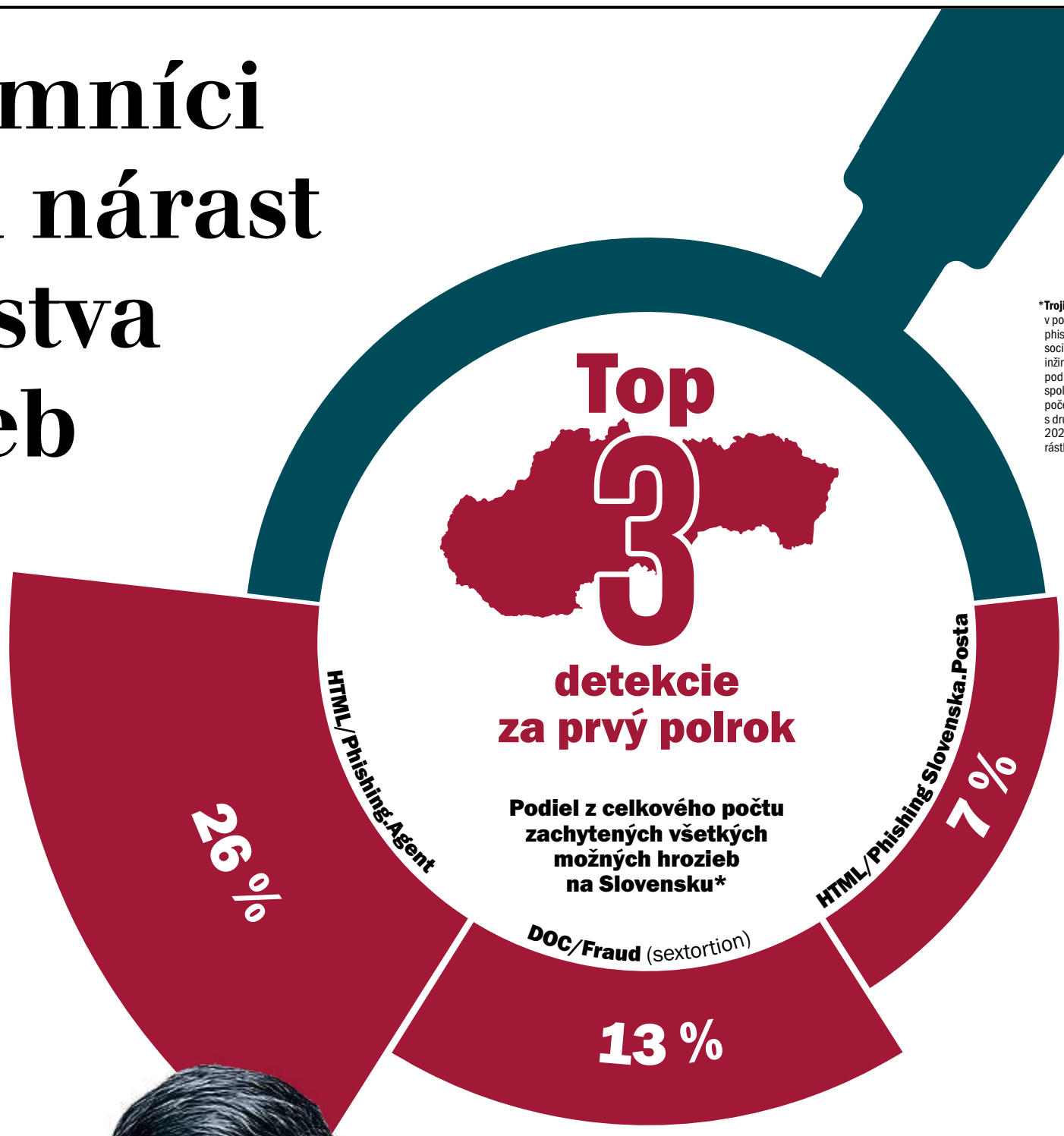
Základom úspechu je dôvera voči predkladateľovi požiadaviek na investície, a to hlavne v oblasti technických opatrení, ktorým manažment veľmi nerozumie. Tu musí byť argumentom okrem zvýšenia bezpečnosti aj nárast výkonnosti a rozšírenie vlastností prevádzky IT. Štatutárovi je potrebné zdôrazňovať, že svoju zákonnú zodpovednosť za kyberbezpečnosť nemôže na nikoho preniesť.

Tomáš Zaťko,
CEO, etický hacker
Citadelo

Ak nezafungovali formálne argumenty, skôr či neskôr príde skúsenosť. Popálenie. Bolesť a jazvy. To funguje zaručene. Je to síce neskoro, ale neskoro je lepšie ako nikdy.

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 28. – 30. JÚLA 2023

Výskumníci hlásia nárast množstva hrozieb



*Trojica hrozieb je v podstate formou phishingu či sociálneho inžinierstva, pričom podľa výskumníkov spoločnosti ESET ich početnosť v porovnaní s druhým polrokom 2022 dramaticky rástla.

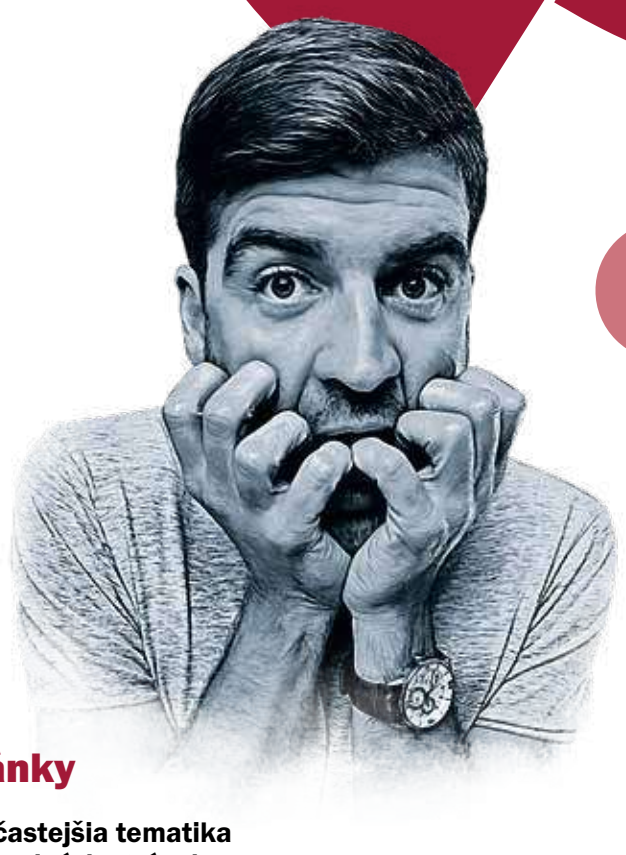
1. Phishingový mail

Škodlivý obsah je bežne distribuovaný ako HTML príloha

Vydáva sa za prihlasovacie okno do balíka MS Office 365 (Outlook, SharePoint)

Nárast:
27 percent

Názov detekcie HTML / Phishing.Agent sa vzťahuje na škodlivé HTML dokumenty odoslané ako prílohy e-mailov. Otvorením prílohy vo webovom prehliadači sa otvorí phishingová stránka, ktorá sa zvyčajne vydáva za poskytovateľa bankových služieb, platieb alebo sociálnych sietí.



2. Podvod zneužíva sexuálnu tématiku

Útočník píše, že si obeť nahral v chúlostivej situácii

Vydiera, že video zverejní, ak obeť nezaplatí 1 500 eur v bitcoinoch

Útočník v skutočnosti nedisponuje kompromitujúcim materiálom

Nárast:
277 percent

V dôsledku nárastu podvodov typu sextortion sa detekcie vrátili na úroveň, ktorá nebola zaznamenaná od roku 2021.

3. Podvod vydávajúci sa za poštu

Útočník zneužíva logo Slovenskej pošty

Mail vyzýva na úhradu poplatku kliknutím na link alebo na prihlásenie do služby

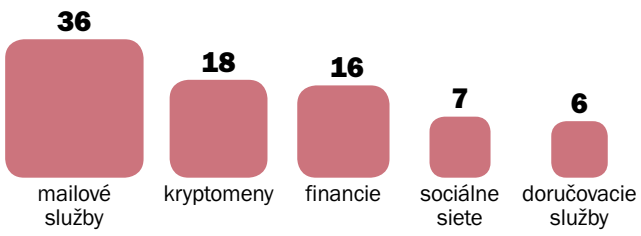
Obeť je presmerovaná na falošnú webovú stránku

Nárast:
275 percent

Phishingové stránky

Za prvý polrok 2023 detegoval ESET
37 -tisíc phishingových stránok

Najčastejšia tematika podvodných stránok (v percentách)



Upozornenie profesionálov

Aktéri hrozieb umiestňujú škodlivé domény do reťazcov presmerovaní, ktoré používajú reklamy na legitímnych webových stránkach. Zvyčajne táto doména presmeruje na potenciálne nežiaducu alebo škodlivú stránku, ktorá obťažuje návštevníkov agresívnou reklamou alebo podvodnými produktmi.

Zdroj: ESET Threat Report, december 2022 – máj 2023

KOMENTÁR

Umelá inteligencia dokáže veľa. Môže maľovať aj na modro?

Rozdelenie na „zlých“ a „dobrých“ sa v kyberbezpečnosti ukotvilo ako rozdelenie na červené tímy a modré tímy. Zlí červení útočia a modrí, tí dobrí, bránia. V posledných dňoch rezonujú obavy, ako červení zneužívajú umelú inteligenciu (AI). Treba si však uvedomiť, že neútočí samotná umelá inteligencia, ale široká dostupnosť nástrojov na tejto báze poskytuje prostriedky útočníkom.

Našťastie ani modré tímy nezaspali dobu. Technologické giganty stojace za poprednými kyberbezpečnostnými platformami mali už dávno dostatočné množstvo dát aj prostriedkov. A ak sa pozrieme na umelú inteligenciu širšou optikou, hovoríme dokonca už o desiatkach rokov skúseností.

Prvky AI sa už dlhodobo a úspešne používajú v biometrických aspektoch autentifikácie používateľov. Analýza správania môže poskytovať rôzne informácie, napríklad kedy si vypýtať dodatočný autentifikačný prvok a naopak – kedy sa dá zo striktných pravidiel ubrať.

Tu si zaslúži samostatnú zmienku behaviorálna analýza. Pri jej využití je vyhodnocovanie udalostí pri sieťovej prevádzke či pri správaní používateľov oveľa adresnejšie, presnejšie a jej účinnosť je neporovnateľná so systémom postavenom na klasických medzných hodnotách. Obrovskou pridanou hodnotou nemusí byť nájdenie konkrétneho prípadu, ale hlavne odfiltrovanie tých nepotrebných. Lebo ak napríklad deväť z desiatich hlásení je irelevantných, vieme sa rýchlo a presne sústrediť na jeden potenciálny problém.

Ďalším príkladom sú bezpečnostné analýzy, kde pracujeme s obrovským množstvo dát, ale aj s informáciami od tretích strán. Tu nám AI uľahčuje prvotné triedenie. Nachádzame tu aj skryté korelácie s dark webom či internetovými fórami. Vyspelé analytické platformy či kyberbezpečnostné nástroje tieto prvky priamo implementujú.

Kontinuálnou úlohou kyberbezpečnosti je aj budovanie znalostnej databázy, ktorá vychádza zo štúdia zraniteľností, hrozieb a správania útočníkov. Čerpať z nej môže aj ten, kto samotným útokom nečelil. Svetoví hráči na poli kybernetickej bezpečnosti využívajú práve AI pri jej tvorbe a distribúcii. V podstate ide o Cybersecurity inteligence, do slovenčiny takmer nepreložiteľný pojem.

Samozrejme, vymenované príklady nemali ambíciu byť vyčerpávajúcim zoznamom. Mali poslúžiť ako ilustračný príklad toho, že hoci sa dnes hovorí o AI hlavne na červenej strane, tak aj špecialisti informačnej bezpečnosti majú tento nástroj v rukách, a čo viac, často s ním dlhé roky už pracujú.

Na druhej strane je nutné si dať pozor na „magické AI nástroje“, ktoré celú kybernetickú bezpečnosť vyriešia za nás. Áno, aj v oblasti kybernetickej bezpečnosti sa nájdu predavači s teplou vodou. Je dobré si preto uvedomiť, že v súčasnosti je AI iba nástroj, a teda výborný pomocník, no špecialistov stále nenahradzuje.

Maľuje teda AI na modro, alebo nie? Podľa môjho názoru umelá inteligencia nielenže maľuje na modro, dokonca používa aj rôzne odtiene modrej.

Michal Srnec,
nadšenec pre kyberbezpečnosť,
CISO Aliter Technologies

Už dnes sme videli budúcnosť

REPORTÁŽ

Východoeurópska letná škola strojového učenia v Košiciach bola udalosťou svetového významu v oblasti umelej inteligencie.

Organizátormi šiesteho ročníka Východoeurópskej letnej školy strojového učenia boli vedci zo spoločnosti DeepMind a spoločnosť ESET. Partnermi boli národná platforma pre rozvoj umelej inteligencie AIslovakIA a Technická univerzita v Košiciach. FOTO: JOZEF KADELA

V auditóriu bolo vyše 250 účastníkov, na pódiu a online sa vystriedali viac ako tri desiatky rečníkov a panelistov. Ak by mala táto vzdelávacia udalosť rating ako hotelové siete, bolo by to päť žiarivých hviezdičiek.

Prémiové podujatie

Na šiesty ročník Letnej školy prišlo viac ako sedemsto prihlášok. „Vybrali sme takú kombináciu účastníkov, aby sme vybalansovali vzdelanie, regióny aj zastúpenie mužov a žien," hovorí Michal Valko z DeepMind, laboratória pre výskum umelej inteligencie spoločnosti Google.

Najlepší ľudia v oblasti umelej inteligencie tu nielen prezentovali, ale aj viedli tutoriály a diskutovali s účastníkmi. „Títo prednášajúci vymysleli algoritmy, ktoré hýbu svetom," zdôrazňuje Michal Valko. Je pôvodom Košičan a dnes pracuje ako výskumník medzinárodných parametrov v oblasti strojového učenia.

Komunita dá viac

Laboratórium DeepMind sa od roku 2010 špecializuje na výskum umelej inteligencie. Tu pracuje trojica výskumníkov Razvan Pascanu, Doina Precup a Viorica Patraucean, ktorí letnú školu založili. Pochádzajú z Rumunska a záleží im na tom, aby mladí ľudia z východnej Európy dostali príležitosť.

Razvan Pascanu hovorí, že sa dá vzdelávať aj online a sám, ale ak ste súčasťou komunity, učíte sa od tých najlepších. Ak máte priamy prístup k najnovším vedomostiam či možnosť stretnúť sa so špičkovými vedcami a vytvoriť si kontakty, napredujete rýchlejšie. Ďalším podnetom pre letnú školu je stav, že východná Európa paradoxne viacej spolupracuje so západoeurópskymi univerzitami ako medzi sebou.

Vystúpiť z komfortnej zóny

Ak si teda organizátori dali cieľ spájať talenty východnej Európy medzi sebou a so svetom, podarilo sa im to nadmieru. V aule Technickej univerzity vznikol výnimočný pracovný mix. V štatistike to bolo 41 krajín zo štyroch kontinentov.

Peter Bakonyi je programátor v kyberbezpečnostnej firme Aliter Technologies a zároveň doktorand na Fakulte informatiky a informačných technológií STU. Najviac oceňuje inšpiratívny rozmer podujatia: „Zrazu vidíte, že k téme sa dá pristupovať aj iným pohľadom a spôsobom."

Aj takto sa to začína

Takmer stovka posterov na Letnej škole znamená takmer stovku nápadov na uplatnenie umelej inteligencie.

Tímy prezentovali výsledky základného výskumu, uplatnenie algoritmov a najviac riešení tu bolo z oblasti zdravotníctva. „Nechceme nahradiť lekárov, chceme im pomáhať. Nech je uplatnenie umelej inteligencie akékoľvek, pod diagnózu sa vždy podpisuje lekár," vysvetľuje Filip Sekerka z Fakulty matematiky, fyziky a informatiky UK. Ako súčasť tímu skúma, ako lepšie a precíznejšie diagnostikovať z CT snímkov nádory na mozgu. Detekcia je časovo náročná a ťažká úloha pre lekárov, nehovoriac o obrovskej zodpovednosti.

Aj v tejto oblasti má však konečné slovo bezpečnosť. Výskumníci tu totiž pracujú so snímkami, ktoré obsahujú osobné údaje, a legislatíva „nestíha" technológiám.

> Títo prednášajúci vymysleli algoritmy, ktoré hýbu svetom.
>
> **Michal Valko,** výskumník DeepMind

Nápad za milión

Pri ďalšom posteri Martin Mocko z Kempelenovho inštitútu predstavuje uplatnenie umelej inteligencie pri analýze škodlivého kódu. Vysvetľuje, ako by to mohlo pomôcť bezpečnostným výskumníkom.

Malvéry, ako ktorýkoľvek iný softvér, môžeme totiž na základe mnohých príznakov zoskupovať do rodín. V súčasnosti počet škodlivých súborov presahuje miliardu, čo znamená aj stovky tisícov príznakov, takže analýza zaberá množstvo času.

Ak však urýchlime analýzu pomocou zhlukovania, urýchli sa aj detekcia a zlepší sa obrana. Voľne povedané, na malvér s podobnými príznakmi sa dá nastaviť presná vakcína ako na chorobu s podobnými príznakmi. Preto sú tieto výskumy už dlhodobo v hľadáčiku tých najlepších technologických firiem.

Toto môžeme zažiť

Hneď druhý deň po posterových prezentáciách sa na pódium postaví Jakub Debski zo spoločnosti ESET a vysvetľuje, ako sa umelá inteligencia aktuálne uplatňuje v kyberútokoch v našom živote a kde sú výzvy, lebo „deepfake sa zmenili na reálne kyberútoky."

Kvalita hlasových deepfake prudko rastie a môže mať desiatky foriem. Tie útočia na naše city, pocit zodpovednosti, alebo – naopak, lakomosť či naivitu.

Predstavte si, že volajú únoscovia, že majú vaše dieťa, a použijú jeho hlas ako dôkaz. Predstavte si, že riaditeľa lokálnej pobočky žiada jeho nadriadený z ústredia o mimoriadny prevod peňazí. Čo urobíte?

Zmena navždy

Akademický prístup je jedna vec, prax druhá. Jakub Debski príkladmi iba začal a pokračuje známou pravdou, že „útoky sa nedejú vedeckým spôsobom". Poukazuje tým na výhodou kyberzločincov, ktorých rozmýšľanie je mimo zavedených pravidiel a etických mantinelov.

Uplatnenie umelej inteligencie zlepšuje texty phishingových mailov, personalizuje útoky a zlepšuje ich škálovateľnosť.

Zároveň, keďže sa generovanie kódu dá presunúť na umelú inteligenciu, útoky okrem toho, že sa zlepšia, ešte budú mať nižšie výrobné náklady. V tejto súvislosti sa začína preto používať aj označenie, že zo softvéru sa stáva zbraň, čiže niečo ako ozbrojovanie alebo militarizácia softvéru.

Tí dobrí a zlí

Ešte nikdy sa svet tak veľa nezaoberal etikou pri vývoji softvéru ako pri uplatnení umelej inteligencie. Takže pre všetkých účastníkov bola magnetom práve prednáška nositeľa Turingovej ceny Yoshuu Bengia. Toto ocenenie je niečo ako Nobelova cena v počítačovej vede, a preto tak silne rezonuje Bengiovo varovanie pred temnými stránkami tohoto vedného odboru.

„Do ochrany verejnosti by sa malo investovať rovnako veľa ako do vývoja umelej inteligencie," hovorí tento populárny vedec. A publikum zastúpené mladými ľuďmi mu nekonečnými otázkami dáva za pravdu.

PORADŇA

Pomôže nám?

Aj keď sme iba malá, či stredná firma, ako nám môže pomôcť umelá inteligencia zlepšiť kyberbezpečnosť?

V najbližších pár rokoch určite uvidíme nespočetné množstvo nových bezpečnostných riešení a nástrojov využívajúcich schopnosti umelej inteligencie. Ich prínosy vidíme už dnes respektíve môžeme v blízkej budúcnosti očakávať v týchto oblastiach

Pri detekcii kybernetických hrozieb: AI dokáže analyzovať veľké množstvá dát vo vysokých rýchlostiach, identifikovať v nich potenciálne hrozby a anomálie, ktoré môžu znamenať kyberútok.

Pri detekcii phishingu: LLM môžu byť natrénované na identifikáciu možných pokusov o phishing, upozorniť užívateľov a správcov na možné hrozby prípadne ich rovno odstrániť.

V automatizácii reakcií na incident: Po detekcii hrozby je kľúčová rýchla reakcia. AI môže automatizovať určité druhy zásahov, napríklad izolovať postihnuté a tak zastaviť šírenie a minimalizovať potenciálne škody.

Pri analýze správania užívateľov: AI dokáže sledovať a analyzovať vzorce správania užívateľov a identifikovať rôzne podozrivé aktivity. Významné odchýlky od zaužívaného „normálu" napríklad neobvyklé prenosy dát môžu spustiť „alarm" a iniciovať podrobnejšiu analýzu.

Pri zlepšovaní bezpečnostného povedomia: AI môže prispieť k vytvoreniu zaujímavejších, interaktívnejších a vierohodnejších školení bezpečnostného povedomia, a posilňovať tak tradične najslabší článok podnikovej obrany – ľudský faktor.

Pri analýze zhody so zákonmi a štandardami: AI bude vedieť špecialistom pomôcť pri posudzovaní zhody s relevantnými zákonmi a predpismi o kybernetickej bezpečnosti. Môže automatizovať kontrolné procesy, signalizovať potenciálne nezhody a vyhnúť sa tak riziku pokút či právnych dôsledkov.

Pri tom všetkom je však dôležité si uvedomiť, že AI nie je a nebude „zázračnou pilulkou" na všetko, a že nenahradí potrebu základných bezpečnostných opatrení. Skôr má potenciál ich vylepšiť a pridať dodatočnú, sofistikovanú úroveň ochrany. Pravidelné aktualizácie softvéru, silné heslá a uvedomelí zamestnanci však nebudú o nič menej dôležití ako kedykoľvek predtým.

Martin Lohnert, Soitron

Otázky posielajte na adresu: **kyberporadna@mafraslovakia.sk**

TREND

Regulácia umelej inteligencie? Je nevyhnutná, aj nebezpečná

V top desiatke najdôležitejších kyberbezpečnostých trendov tejto dekády figuruje aj zneužitie umelej inteligencie.

Európska agentúra pre kybernetickú bezpečnosť ENISA v aktuálnej štúdii upozorňuje najmä na vytváranie sofistikovaných dezinformačných kampaní s použitím nástrojov umelej inteligencie. S umelou inteligenciou však úzko súvisia aj iné riziká – rozširovanie digitálneho špehovania a strata súkromia. Regulácia sa preto javí ako nevyhnutná. Musí však byť citlivá a vyvážená.

Podvody a propaganda

Technologické schopnosti štátov, organizovaného zločinu, ale aj jednotlivcov z radov hackerov, ktorých si môžu najať bežní občania, sa budú rozširovať. Až tak, že prakticky nikto nebude mať problém uskutočňovať pokročilé dezinformačné kampane – či už s finančnými, alebo politickými cieľmi.

Deepfake a novovznikajúce nástroje na báze AI technológie, akými sú Magisto, Animoto, Deep Art Effects, Auphonic, Versus a ich vzájomné kombinácie uľahčujú tvorbu multimediálneho obsahu. Zohrajú rolu pri tvorbe presvedčivých videí a hlasových nahrávok, ale aj pri vytváraní personalizovaných odpovedí či reakcií v diskusiách, čo je kľúčová časť informačných kampaní na sociálnych sieťach.

Vylepšenie techník

Pri takzvanom spear phishingu poslúži AI na okamžitú analýzu verejne dostupných údajov. Následne potom na vytváranie špecifických útokov zameraných na odcudzenie veľmi citlivých dát, až do úrovne biometrických identifikátorov.

Ďalším rizikom AI je manipulácia algoritmov založených na strojovom učení s cieľom ovplyvniť automatizované rozhodnutia informačných systémov používaných širokou verejnosťou, čo bude spadať pod veľmi sofistikované útoky cez dodávateľské reťazce.

Až príliš veľa údajov

ENISA upozorňuje aj na nástup AI v súvislosti s možnosťami sledovania polohy, s údajmi z kamerových systémov, so zvýšeným dohľadom nad sociálnymi médiami, s biometrickými technológiami na identifikáciu osôb a s konceptom digitálnych identít. Tieto kombinácie údajov môžu viesť k obmedzovaniu osobných slobôd, a to paradoxne z dôvodu zvýšenia bezpečnosti a ochrany spoločnosti.

Rozsiahle dátové úložiská vytvárané bezpečnostnými službami a orgánmi činnými v trestnom konaní sa zároveň bezpochyby stanú atraktívnymi cieľmi pre organizovaný zločin. Ten, ktorý už dnes čulo obchoduje s osobnými údajmi získanými z rôznych online zdrojov.

Európa sa preberá

Možností zneužitia umelej inteligencie v kyberpriestore je oveľa viac. Otázky regulácie a usmerňovania AI sú preto nielen opodstatnené, ale aj naliehavé. Minimálne v Európskej únii je ich na stole niekoľko.

Pozornosť si zaslúži najmä Artificial Intelligence Act., teda regulácia umelej inteligencie, ktorej cieľom je nastavenie rámcov a zabezpečenie podmienok na vývoj a používanie tejto inovatívnej technológie. Cyber Ressilience Act. navrhuje reguláciu a zlepšenie kyberbezpečnosti a kyberodolnosti v EÚ prostredníctvom spoločných noriem kyberbezpečnosti pre produkty s digitálnymi elementmi vrátane prvkov umelej inteligencie.

Prísľubom regulácie je vytvorenie etických rámcov a presadzovanie transparentnosti a zodpovedného prístupu. Cieľom je lepšia ochrana súkromia a zvýšenie dôvery verejnosti voči AI. Problémom môže byť príliš rýchly technologický rozvoj, s ktorým regulátori nedokážu udržať krok, či globálne presadzovanie pravidiel, kde je nevyhnutná nadnárodná spolupráca a harmonizácia.

Nástrahy regulácie

Zle navrhnutá regulácia však môže mať aj neočakávané, nechcené následky a byť dokonca škodlivá. Ak budú pravidlá príliš striktné alebo vytvoria priveľké bremeno pre menšie firmy, udusia inovácie a budú brzdiť vývoj užitočných aplikácií. Zároveň to môže centralizovať moc a kontrolu do užšieho spektra konsolidovaných subjektov – či už štátov, politických zoskupení alebo nadnárodných korporácií.

V neposlednom rade – definovať univerzálne prijateľné etické štandardy môže byť mimoriadne zložité, keďže kultúrne, sociálne a geopolitické rozdiely generujú výrazne odlišné názory a spoločenské normy v jednotlivých krajinách.

Roman Čupka, hlavný konzultant spoločnosti Progress