HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
24. – 26. FEBRUÁRA 2023

Partneri špeciálnej prílohy:
ALISON
ALITER TECHNOLOGIES

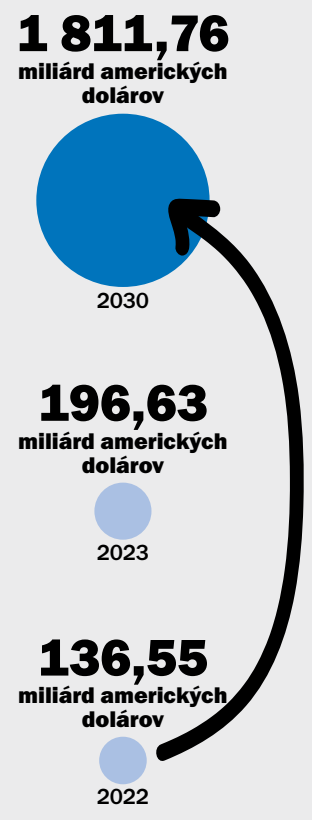
Umelá inteligencia nám rozumie. To nie je iba fakt, to je varovanie

TÉMA

S využitím umelej inteligencie žijeme už desiatky rokov. Všeobecný ošiaľ však nastal, keď sa začala s nami „rozprávať“. Máme pocit, že nám rozumie. To áno.

V súčasnosti až 77 percent elektronických zariadení, ktoré používame, využíva niektoré z prvkov umelej inteligencie. FOTO: DREAMSTIME

HODNOTA GLOBÁLNEHO TRH S UMELOU INTELIGENCIOU
(softvér, hardvér a služby)



Tak si teraz predstavte, že máte prístup ku všetkým faktom zhromaždeným na internete. Zároveň viete, ako informácie súvisia, ako sa podobný problém riešil a aký to malo dosah. A to všetko viete zistiť nepredstaviteľnou rýchlosťou a ešte aj pekne povedať. Tak nejako pracuje populárny nástroj ChatGTP, ktorý zaberá päť najväčších superpočítačov vo svete.

Najslávnejší startup

V januári bolo výskumné laboratórium OpenAI ohodnotené na 29 miliárd dolárov. Cesta od nuly k súčasnej cene mu trvala iba sedem rokov a jeden mesiac.

OpenAI rozpútal súboj technologických gigantov a z vedy urobil hit. Umelá inteligencia je však predovšetkým príležitosť pre firmy, vzdelávanie a nové profesie.

Riešenie sa ponúka

Na Slovensku je 160-tisíc záujemcov o zamestnanie a 82-tisíc otvorených pozícií. A určite musí byť spôsob, ako sa vzájomne nájdu tí praví, aby pasovali požiadavky, termíny aj náklady.

Startup Jobno.one používa umelú inteligenciu na prečítanie životopisu a jeho porovnanie s otvorenou pozíciou. A naopak. Záujemca nahrá životopis na portál, systém mu o pár sekúnd zobrazí otvorené pozície zoradené podľa zhody. Stačí kliknúť a inzerent otvorenej pozície dostane informáciu o záujemcovi do interného systému.

Drina každý deň

Od prvej myšlienky k veľkým investíciám to chlapcom z Jobno.one trvalo päť rokov. V minulom roku však prišlo 1,6 milióna eur a teraz testujú OpenAI a ChatGPT ako alternatívu k Azure AI, ktoré používajú. Systém je navrhnutý tak, že umelá inteligencia nesmie analyzovať vek, pohlavie, orientáciu či svetonázor. Porovnávajú sa iba schopnosti, skúsenosti a vzdelanie. „Máme takzvanú bias-free, čiže technológiu bez predpojatosti. V tom sme zatiaľ jedineční,“ vysvetľuje Jozef Belvončík.

Vizionársky nákup

Spoločnosť Ixperta investovala do startupu Sentisquare už v roku 2016. Reagovala tým na fakt, že kontaktné centrá dlhodobo trpia nedostatkom ľudí a ich význam bude rásť.

Vývojári nielenže učia stroj ľudskej reči, ale idú ešte ďalej. Naučili ho pochopiť kontext a vycítiť náladu zákazníka. Operátori v kontaktných centrách tak môžu použiť odporúčanú odpoveď a výrazne sa skracuje čas na spracovanie požiadavky zákazníka.

Ako však zo skúseností hovorí Andrej Kavický, na Slovensku stále narážajú na pasívne odmietanie takýchto riešení, v čom sa líšime od susedného Česka.

Jasná línia od začiatku

Aj keď je umelá inteligencia momentálne opäť na výslní, v bankovníctve nie je ničím novým. Príklady vidíme už desiatky rokov v digitalizácii a extrakcii informácií z dokumentov, v robotizácii alebo dokonca aj v elektronickom podpisovaní.

Ako ďalšiu úlohu si preto dali v Tatra banke pomáhať zákazníkom so správou ich financi, a preto každému dožičia v blízkej budúcnosti „virtuálneho finančného poradcu“.

Manažér dát a inovácií Daniel Minárik tu však zdôrazňuje, že kým dostanú zákazníci technológiu k dispozícii, prebieha hĺbková analýza možných dosahov. „Zodpovedná komunikácia v oblasti umelej inteligencie a edukácia zákazníkov a zamestnancov je to, čo nás odlišuje v rámci konkurenčného prostredia.“

> Ľudia väčšinou dobrovoľne odovzdávajú dáta prostredníctvom sociálnych sietí, smart telefónov či hodiniek.
>
> **Jozef Bálint,** bezpečnostný špecialista Alison Slovakia

Rovnako aj o chatbota Adama, ktorý je v prevádzke viac ako tri roky sa stále stará tím odborníkov, ktorý dohliada na to, na akých dátach sa učí, koľko toho vie a čo odpovedá.

Veľmi citlivá oblasť

Pavol Helebrandt vedie na Fakulte informatiky a informačných technológií STU výskumnú skupinu zameranú na kyberbezpečnosť a siete.

„Jednoduchšie štatistické a heuristické metódy v bezpečnosti sa začali používať V 90. rokoch,“ vysvetľuje. Dnes sa za umelú inteligenciu často považujú až výpočtovo náročnejšie techniky s úzko špecifickým zameraním, ako sú napríklad neurónové siete.

Tieto techniky sú postupne nasadzované približne od roku 2016 do rôznych bezpečnostných produktov a riešení, akými sú firewally či systémy na detekciu prieniku. Systémy na detekciu prieniku sa už „naučili“, ako vyzerá štandardná sieťová prevádzka, a vedia odhaliť anomálie alebo neštandardné správanie, napríklad skenovanie portov útočníkom.

Aj vy ju trénujete

S technologickým rozmachom, rastúcim počtom IoT a smart zariadení či cloudových služieb je využívanie metód strojového učenia čoraz sofistikovanejšie. Pre umelú inteligenciu takto vznikajú obrovské data sety, z ktorých sa dokáže učiť.

A navyše? „Ľudia väčšinou dobrovoľne odovzdávajú dáta prostredníctvom sociálnych sietí, svojich smart telefónov, hodiniek, domácností a smart všetkého,“ vysvetľuje bezpečnostný špecialista Jozef Bálint zo spoločnosti Alison Slovakia.

Prémiová premiéra

Keď bol nástroj ChatGTP koncom roka 2022 uvoľnený pre širokú verejnosť, jeho schopnosti mnohým doslova „vyrazili dych“, hovorí Michal Srnec, CISO spoločnosti Aliter Technologies.

To, čo vyrazilo dych profesionálom, je možnosť využiť nástroj v kybernetickej bezpečnosti. Takáto implementácia umelej inteligencie môže byť totiž použitá na hľadanie zraniteľností v kóde či písanie samotného škodlivého kódu.

Schopnosť generovať text v takmer ľubovoľnom jazyku vytvára priestor na masívnu tvorbu takzvaných spear phishingových kampaní. Takto dobre napísaný phishingový mail má vierohodnú formuláciu, ľudským pohľadom len veľmi ťažko rozoznateľnú.

Zákon o umelej inteligencii

Advokát so špecializáciou na IT právo a moderné technológie Miroslav Chlipala poukazuje na celoeurópsku jednotnú reguláciu. V závislosti od rizika umelej inteligencie bude daná aj miera jej regulácie. A pridáva aj príklady.

Medzi zakázané systémy budú patriť hračky s hlasovým asistentom, ktoré nabádajú na nebezpečné správanie. Do prísne regulovaných systémov sa radí softvér triediaci životopisy na účely ďalšieho výberu. Skupinu s obmedzeným rizikom budú tvoriť chatboti, kde bude povinnosť informovať používateľa o tom, že komunikuje s neživou bytosťou. Neobmedzené používanie umelej inteligencie bude pri videohrách a spamových filtroch.

Rozozná stroj dobro a zlo?

Dokáže stroj chápať, čo je správne a čo nie? Od odpovedí závisí, či rozvoj kognitívnych systémov bude pre kybernetickú bezpečnosť prínosom alebo hrozbou. Teda či sa budeme stretávať v budúcnosti častejšie s robotom, ktorý útočí, alebo s robotom, ktorý chráni.

„Čo sa týka bezpečnosti, v súčasnosti tu vidím umelú inteligenciu ako doktora Jekylla a zároveň pána Hyda zo slávneho hororu o protikladoch ľudskej povahy,“ hovorí Ivan Makatura z Kompetenčného a certifikačného centra kybernetickej bezpečnosti. A pridáva svoj povestný citát: „Nateraz je vážnym problémom ešte stále iba ľudská hlúposť, a nie umelá inteligencia.“

ANKETA MESIACA: BEZPEČNOSTNÍ PROFESIONÁLI VÁM VYSTAVILI VYSVEDČENIE

Zmenilo sa vnímanie a stav kybernetickej bezpečnosti rok po invázii? Aké ponaučenie sme si zobrali, kto čo urobil a čo sa stane tomu, kto zaspal.

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 24. – 26. FEBRUÁRA 2023

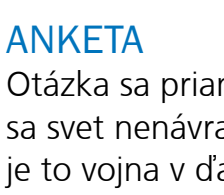
Profesionáli vám vystavili vysvedčenie

ANKETA

Otázka sa priamo ponúka. V uplynulom roku sa svet nenávratne zmenil a my už vieme, čo je to vojna v ďalšej dimenzii. Preto sa pýtame, či sa zmenilo aj vnímanie a stav kybernetickej bezpečnosti rok po invázii. Aké ponaučenie sme si zobrali, kto čo urobil a čo sa stane tomu, kto zaspal dobu.

Ivan Makatura,
generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Nazval by som toto obdobie premárnenou šancou. Nepadajú tu síce bomby, ale v kyberpriestore zúri skutočná vojna. A my namiesto toho, aby sme uplatnili reálne nástroje obrany proti kybernetickým hrozbám a cielenej propagande zo strany nepriateľského štátu, nechávame voľný priestor kolaborantom. Naši dedovia sa musia obracať v hroboch.



Roman Čupka,
hlavný konzultant
Progress Software
a CEO Synapsa Networks

Invázia nemala veľký vplyv na budovanie kybernetickej bezpečnosti v organizáciách. Hlavnými motiváciami zostávajú regulácie, legislatíva, ochrana zákazníkov, používateľov a služieb. Rovnako pretrvávajú aj najväčšie prekážky kvalitného zabezpečenia – nedostatok špecialistov a zdĺhavé implementácie komplexných nástrojov. Zlepšilo sa však vzdelávanie a povedomie, a to aj na úrovni manažmentu, čo je dôležitý krok k úspechu.

Tomáš Zaťko,
CEO, etický hacker
Citadelo

Aj v kybernetickej bezpečnosti platí, že v zlých časoch si ľudia jasnejšie uvedomujú, že môže byť zle. Ale v tých dobrých časoch sa na to lepšie pripravuje. Zároveň – vždy môže byť horšie. Dúfajme v najlepšie. Pripravujme sa na najhoršie.

Paula Babicová,
zodpovedná za ochranu osobných údajov
Dôvera, zdravotná poisťovňa

Zdravotníctvo je neustále terčom kybernetických útokov, a to bez ohľadu na aktuálnu geopolitickú situáciu vo svete. Riziká vnímame rovnako intenzívne aj rok po invázii, výrazné zmeny nenastali. Stále sa snažíme v našej spoločnosti robiť čo najviac najmä vo vzdelávaní a investujeme veľa úsilia v tejto oblasti aj v celom sektore zdravotníctva.

Andrej Žucha,
generálny riaditeľ
ALISON Slovakia

Profíci spozorneli a bili na poplach, manažment väčšinou zaujal vyčkávaciu pozíciu a robil iba nevyhnutné minimum, a politici robili, čo im ide najlepšie: rozprávali o tom a robili nič.

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

V kybernetickom priestore je badať intenzívnejšie vedenie útokov. Nielen útoky na infraštruktúru, ale aj spôsoby vedenia a šírenia falošných informácií cez sociálne siete. Na odvrátenie takéhoto stavu nemusíme vymýšľať koleso, ale stačí robiť to, čo v informačnej či kybernetickej bezpečnosti už platí roky. Štát by mal začať reálne a bezpodmienečne investovať nielen do kvalitnej infraštruktúry, ale hlavne do ľudí.

Róbert Mramúch,
manažér kybernetickej bezpečnosti
MH Teplárenský holding

V našej brandži platí staré dobré – čert nikdy nespí. Preto netreba zaspať na vavrínoch. Dojem, že keď sa nám za rok nič nestalo, zajtra to nemôže byť inak, je mylný. Úroveň zabezpečenia v kybernetickom priestore sa mení každým nastavením či novou konfiguráciou. Úlohou nás, bezpečákov, hoci nás je na Slovensku ako šafranu, je vyhodnocovať a neustále upozorňovať na možné hrozby.

Diana Legdanová,
vedúca úseku bezpečnosti
Východoslovenská energetika Holding

Strach je silný motivátor, preto verím, že vnímanie kyberbezpečnosti sa výrazne zmenilo. Je otázne, či sa dostatočne zmenilo aj samotné správanie jednotlivcov či zodpovedné konanie organizácií. Ešte stále veľa organizácií na Slovensku je v reaktívnej fáze vyspelosti kultúry kyberbezpečnosti, a teda „čaká sa na prúser“, kým sa zmenia priority. Tí rozumní majú zabezpečenú ochranu, back-up aj obranu.

Rastislav Janota,
riaditeľ
Národné centrum kybernetickej bezpečnosti SK-CERT

Inváziu Ruska na Ukrajinu priniesla nárast útokov aj v slovenskom kybernetickom priestore a povedomie firiem a inštitúcií o kybernetickej bezpečnosti sa mierne zvýšilo. Najmä v tých väčších. Menšie firmy stále vytrvalo ignorujú ohrozenie. Okrem výnimiek ani vo verejnej správe nevnímame viditeľný pokrok v oblasti zvyšovania odolnosti. Stále prevažujú výhovorky pred skutočnými činmi.

Lukáš Okál,
manažér rozvoja bezpečnostných služieb
Microsoft Česká republika a Slovensko

Vnímanie kybernetickej bezpečnosti má vyššiu prioritu. Organizácie všetkých typov sa denne stretávajú s informáciami, kto bol za posledných pár hodín terčom kybernetického útoku. Neustále sa stretávame s novými hrozbami, a preto treba reagovať pružne. Meníme sa aj my dodávatelia a korporácie a kybernetická bezpečnosť našich zákazníkov pre nás nadobúda čoraz vyššiu prioritu.

Ivan Kopáčik,
bezpečnostný expert
Gordias

Aj naša krajina zažila a zažíva kybernetické útoky v dôsledku faktu, že figurujeme na zozname nepriateľských krajín. Za týmito útokmi však už nestoja bežní kyberútočníci, ale profesionáli. V dôsledku toho sme nútení zamyslieť sa aj nad rizikami, ktoré sme doteraz neriešili, napríklad prieniky v dôsledku zverejnenia zdrojových kódov štátnych informačných systémov.

Marián Trizuliak,
architekt kybernetickej bezpečnosti
Západoslovenská distribučná

„Nie, toto sa nestane, veď to je vylúčené...“ – a došlo vytriezvenie. Rovnako ako v oblasti diplomacie, aj v kybernetickej bezpečnosti sme zostali šokovaní, nie zaskočení. Veci dovtedy nepravdepodobné a nemožné sa stali skutočnosťou. Riziká, doteraz označované ako nepravdepodobné, sa stali skutočnými. Riadenie kontinuity a obnovy v prípade katastrofy sa zjavne stalo hlavnou témou mnohých krízových manažérov. Všetko zlé je na niečo dobré.

Ján Grujbár,
generálny riaditeľ
Aliter Technologies

Kybernetická bezpečnosť sa dostala na rokovací stôl a práve invázia na Ukrajinu tento posun výrazne zrýchlila. Oveľa väčšia časť spoločností si naplno uvedomuje jej dôležitosť a zohľadňuje ju pri svojich strategických, ale aj každodenných rozhodnutiach. Sme však len na začiatku – ťažká práca nás ešte len čaká. Schválený rozpočet a uvedomenie je jedna vec, no správne nasadenie a následná operatíva je úplne iná vec.

Štefan Mizerák,
manažér oddelenia IT bezpečnosti
NN Životná poisťovňa

Počet a intenzita kyberútokov sa za posledný rok zvýšili niekoľkonásobne, štátom sponzorované kampane sú mierené na vládne inštitúcie a aj súkromný sektor. Tento trend naznačuje, ako bude vyzerať príprava a vedenie budúcich konfliktov, kyberútoky sú súčasťou vedenia vojny s dosahom na spoločnosti. Firmy na Slovensku posilňujú kyberodolnosť a snažia sa byť pripravené lepšie než pred rokom.

Richard Kiškováč**,**
generálny riaditeľ
Elkan

Rok po invázii v stave kybernetickej bezpečnosti nedošlo k žiadnym dramatickým zmenám. V podstate môžeme povedať, že kto sa systematicky venoval zvyšovaniu úrovne kybernetickej bezpečnosti, ten pokračoval v tomto úsilí. Kto tak nerobil, za také krátke obdobie toho veľa nemohol stihnúť. Je potrebné si uvedomiť, že budovanie bezpečnosti je vždy naviazané na rozpočtovacie cykly a len málokedy sa nájdu dodatočné, čiže neplánované zdroje.

Ján Adamovský,
riaditeľ bezpečnosti
Slovenská sporiteľňa

Po prvotnej panike spôsobenej faktom, že vojna sa naozaj začala, sa situácia upokojila. Obrovské hrozby, ktoré sme v kybernetickom priestore nášho regiónu očakávali, sa nenaplnili. Pre mňa však zostáva obrovskou zmenou skutočnosť, že predtým sme rátali s útokmi motivovanými peniazmi, konkurenčnou výhodou alebo snahou získať dáta. Teraz musíme rátať s tým, že nastanú útoky s jediným cieľom – čo najviac zdevastovať spoločnosť, ideálne ju prostredníctvom kybernetických útokov kompletne zničiť. Bez ďalšej vedľajšej motivácie.

Tomáš Valenta,
riaditeľ
Check Point Software Technologies na Slovensku

Invázia poukázala na zraniteľnosť štátov a kritickej infraštruktúry. Štáty, ktoré porozumeli tejto hrozbe, zvýšili opatrenia investíciami do nových technológií a rozšírením kyberbezpečnostných tímov. Na medzinárodnej úrovni sa prehlbuje spolupráca, zdieľanie informácií a rozvíjajú sa spoločné reakcie na kybernetické útoky. Zvýšilo sa aj povedomie o dôležitosti kybernetickej bezpečnosti, ktorá úzko súvisí s tou národnou.

Henrich Šnajder,
manažér IT bezpečnosti
Orange Slovensko

Po inváznii sa na Slovensku zvýšilo povedomie o kybernetickej bezpečnosti. Krajina sa snaží zlepšiť obranu a investovať do ochrany kritických systémov. Viac prípadov kybernetických útokov viedlo k zlepšeniu spolupráce vlády a súkromného sektora. V roku 2022 schválili nový zákon, ktorým sa zlepšila regulácia a ochrana informačných systémov pred kybernetickými hrozbami a definujú sa nové postupy na zabezpečenie kritických infraštruktúr.

Michal Ďorda,
audítor kybernetickej bezpečnosti
Auditori.it

Počet kybernetických útokov v niektorých krajinách sa po začatí vojny až strojnásobil. Môžeme preto povedať, že na koho hackeri ešte neútočili, ten akoby ani neexistoval. Samotné inštitúcie preto viac začali sledovať, čo sa deje v kyberpriestore okolo nich, ako to môže ovplyvniť ich biznis, čo vedia urobiť pre zníženie existujúceho rizika, ale hlavne kde na to zobrať finančné prostriedky. Ak „osvieti“ všetkých manažérov KB, úroveň bezpečnosti o rok bude ešte vyššia, ako je aktuálne.

Tomáš Hettych,
viceprezident
ISACA

Vnímanie sa zmenilo dramaticky. Kybernetická bezpečnosť už nie je okrajová téma pre riaditeľov organizácií alebo majiteľov firiem. Hrozby, zraniteľnosti, útoky sa objavujú takmer denne. Túto tému už nikto neodsúva na okraj svojho záujmu. Rok 2023 je rok veľkého množstva opakovaných auditov kybernetickej bezpečnosti. Chcem veriť, že aj reálny stav kyberbezpečnosti sa zlepšil a miera súladu poskytovateľov základných služieb sa markantne zvýšila.

Martin Lohnert,
riaditeľ centra kybernetickej bezpečnosti
Void SOC Soitron

Pri hrôzach, ktoré sa na Ukrajine dejú, je vlastne prekvapujúce, že ešte stále neprišlo k útokom, ktoré by spôsobili rozsiahle výpadky kritickej infraštruktúry alebo nezvratné poškodenie štátnych či súkromných organizácií. Pri polemizovaní, ako je to možné, stačí, keď si spomenieme na ukrajinské skúsenosti s NotPetya z 2017. Zrejme naozaj platí, že „šťastie praje pripraveným“. My ostatní, pre ktorých najväčšie kybernetické ohrozenie stále predstavujú finančne motivovaní zločinci, by sme na to nemali zabúdať.

Kristína Urbanová,
špecialistka informačnej bezpečnosti
ESET

Udalosti na Ukrajine do mnohých myslí zaniesli dosiaľ abstraktné otázky zabezpečenia kontinuity činnosti v čase krízy. Organizácie sa hlbšie zapozerali do svojich vnútorných procesov. Postupne identifikovali, ktoré systémy sú kostrou ich fungovania a vzhľadom na aktuálny scenár zvyšujú ich odolnosť. A v neposlednom rade začali rozmýšľať nad tým, ako udržať svojich ľudí v bezpečí.

Pavel Nechala,
advokát
Nechala and partners

Invázia Ruska na Ukrajinu je od začiatku sprevádzaná útokmi v kyberpriestore v snahe oslabiť druhú stranu. Doterajší priebeh potvrdil, že kolektívna spolupráca a podpora, výmena skúseností a vedomostí môže zmeniť očakávania výsledku. Napriek masívnym útokom na Ukrajinu a susedné štáty sa podarilo spoluprácou západných krajín a súkromných spoločností vrátane slovenských vybudovať odolnú infraštruktúru proti ruským malvérom.

Dominik Procházka,
riaditeľ odboru bezpečnosti
AGEL SK

Súčasne s konfliktom na Ukrajine prebiehajú aj neustále kybernetické útoky. Kybernetická bezpečnosť dnes zaujíma každého. V rámci organizácie zaznamenávame významný nárast hlásených udalostí, to je dobré. Vnímanie kybernetickej bezpečnosti ako celku, do ktorého môže prispieť každý, je znakom toho, že ľuďom nie je bezpečnosť ľahostajná a chcú pomôcť. Odkladať opatrenia nemá v spoločnostiach miesto, zaváhanie môže spôsobiť kolaps.