Pri posilňovaní kybernetickej obrany Európy sú AI a postkvantová bezpečnosť kľúčové

SLOVENSKÁ SPOLOČNOSŤ ROZVÍJA TECHNOLÓGIE NA OCHRANU KRITICKEJ INFRAŠTRUKTÚRY, VESMÍRNYCH SYSTÉMOV A OBRANNÉHO PRIEMYSLU

Firma Decent Cybersecurity sa etablovala ako líder v oblasti kybernetickej bezpečnosti s dôrazom na obranný priemysel, kritickú infraštruktúru a vesmírne systémy. Spolupracuje s organizáciami ako NATO, European Space Agency či European Defence Fund na vývoji pokročilých bezpečnostných riešení. Ako firma využíva umelú inteligenciu a postkvantovú kryptografiu na ochranu strategických systémov, aké hrozby čakajú európsku kybernetickú bezpečnosť a prečo je nevyhnutná technologická suverenita – aj na tieto otázky odpovedá zakladateľ, generálny riaditeľ a predseda predstavenstva Matej Michalko a zakladateľka a COO (prevádzková riaditeľka) spoločnosti Decent Cybersecurity Michaela Abel.

Decent Cybersecurity je významným hráčom v oblasti kybernetickej bezpečnosti s dôrazom na zbrojárstvo, kritickú infraštruktúru a vesmírne systémy. Aké projekty a partnerstvá považujete za najvýznamnejšie?

MM: Naša cesta bola od začiatku jasne zameraná na najnáročnejšie oblasti kybernetickej bezpečnosti – vesmírny priemysel, obranu a kritickú infraštruktúru. Za kľúčové považujem najmä strategické partnerstvá s Agentúrou NATO pre podporu a obstarávanie (NATO Support and Procurement Agency) a Európskou vesmírnou agentúrou (European Space Agency), ktoré potvrdzujú našu expertízu na najvyššej úrovni. Získanie bezpečnostnej previerky na stupeň „tajné" pre NATO a Európsku úniu (EÚ) bolo významným míľnikom, ktorý nám otvoril dvere k najdôležitejším projektom v oblasti európskej obrany. Spolupráca s lídrami ako Thales, Leonardo či Norwegian Defence Research Establishment (Nórsky výskumný ústav obrany) nám umožňuje prinášať skutočne inovatívne riešenia v oblasti postkvantovej kryptografie a blockchainovej bezpečnosti. Takisto sme členom Združenia bezpečnostného a obranného priemyslu SR a zakladajúcim členom Asociácie kritickej infraštruktúry Slovenskej republiky, teda združenia, ktoré sa zaoberá problematikou kritickej infraštruktúry a základných služieb.

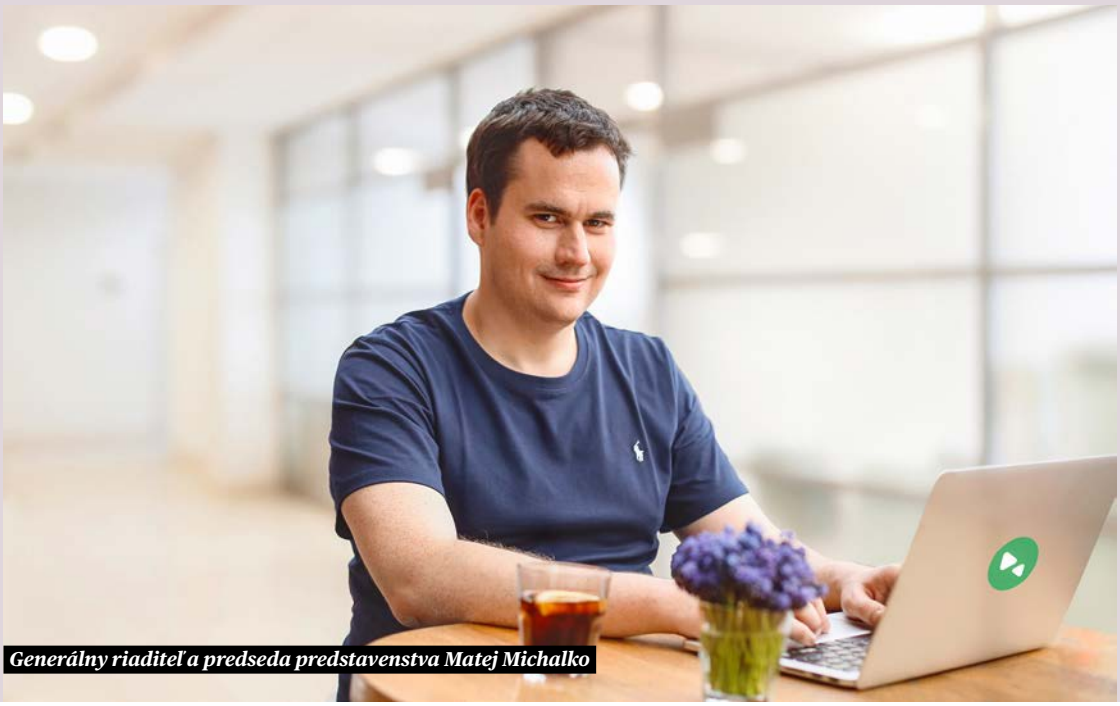
TREND
WE KNOW HOW

V rámci Európskeho obranného fondu ste zapojení do 32-miliónového projektu. Aký je váš prínos a čo tento projekt znamená pre budúcnosť kybernetickej bezpečnosti v Európe?

MM: Projekt AIDA predstavuje prelomovú iniciatívu v oblasti európskej kybernetickej obrany. Náš tím sa špecificky zameriava na vývoj pokročilých AI agentov, ktoré dokážu autonómne detegovať a reagovať na kybernetické hrozby. Je to významný posun od tradičných reaktívnych prístupov k proaktívnej obrane. Hodnota projektu vo výške 32,45 milióna eur, z čoho 26 miliónov poskytuje EÚ, podčiarkuje jeho strategický význam. Spolupracujeme s 23 špičkovými európskymi organizáciami počas 42 mesiacov na vytvorení systému, ktorý významne posilní európske obranné spôsobilosti.

Kvantové počítače predstavujú hrozbu pre súčasné šifrovacie systémy. Ako konkrétne pripravujete svoje riešenia na éru postkvantovej kryptografie?

MM: Postkvantová bezpečnosť je pre nás absolútnou prioritou. Už dnes implementujeme NIST – schválené postkvantové algoritmy, do našich kľúčových produktov. Napríklad náš



Generálny riaditeľ a predseda predstavenstva Matej Michalko

Foto – Emil Vaško

COO (prevádzková riaditeľka) Michaela Abel

QuantumProof Protocol využíva kombináciu lattice-based kryptografie a pokročilých hash-based podpisových schém. Aktívne modernizujeme existujúce systémy našich klientov tak, aby boli kvantovoodolné. Skúmame a vyvíjame aj vlastné algoritmy.

Aké sú najväčšie kybernetické hrozby pre obranný a zbrojársky sektor v najbližších piatich rokoch?

MM: Vidíme tri hlavné trendy. Prvým je rastúca sofistikovanosť state-sponsored útokov, ktoré často kombinujú tradičné hekerské techniky s pokročilou umelou inteligenciou. Druhým je ohrozenie dodávateľských reťazcov – útočníci sa zameriavajú na menšie firmy v dodávateľskom reťazci, aby sa dostali k väčším cieľom. Tretím je práve quantum computing threat. Špecifickou výzvou je ochrana systémov na riadenie bezpilotných prostriedkov a vesmírnych zariadení. Ide o zabezpečenie spoľahlivej autentifikácie, dôvernosti, dostupnosti a integrity prenášaných dát v reálnom čase.

Nedávne kybernetické útoky na kataster a Všeobecnú zdravotnú poisťovňu poukázali na slabiny štátnej IT infraštruktúry. Ako hodnotíte úroveň kybernetickej ochrany Slovenska a čo považujete za najväčšie nedostatky?

MM: Tieto incidenty jasne ukazujú, prečo je kybernetická bezpečnosť kriticky dôležitá pre každodenný život občanov. Keď občan nemôže vybaviť niečo na katastri, dotkne sa ho to. Keď dôchodcom neprídu načas dôchodky pre ransomvérové útoky na Sociálnu poisťovňu, dotkne sa ich to. Tomuto chceme predchádzať. Ako zakladajúci člen Asociácie kritickej infraštruktúry Slovenskej republiky a dlhoročný člen Združenia bezpečnostného a obranného priemyslu SR aktívne pracujeme na zlepšení tejto situácie.

V ktorých konkrétnych vesmírnych programoch sa vaše technológie už využívajú alebo sa pripravujú na nasadenie?

MM: Naše technologické riešenia sú aktívne implementované v rámci významných medzinárodných vesmírnych programov. Podieľame na vývoji a implementácii quantum-safe komunikačných protokolov pre novú generáciu satelitov. Významným míľnikom je náš vlastný projekt SecureSat Guardian, ktorý poskytuje komplexnú ochranu satelitných komunikácií pred súčasnými aj budúcimi kvantovými hrozbami. Paralelne s tým vyvíjame blockchain-based systémy pre bezpečnú výmenu orbitálnych dát, čo predstavuje kritický komponent pre efektívne riadenie vesmírnej prevádzky. Aktívne sa podieľame aj na programoch zameraných na ochranu kritickej vesmírnej infraštruktúry v spolupráci s európskymi partnerskými organizáciami.

Náš prístup je založený na implementácii medzinárodných štandardov NATO a EÚ, pričom kladieme dôraz na modulárnu architektúru našich systémov

Ako dokážete udržiavať inovácie pri práci v takých prísne regulovaných sektoroch, akým je obrana, vesmír a kritická infraštruktúra?

MA: Inovácie v prísne regulovaných sektoroch vyžadujú jedinečný prístup, ktorý vyvažuje potrebu rýchleho technologického pokroku a dodržiavanie prísnych bezpečnostných štandardov. Vytvorili sme špecializované vývojové tímy, ktoré úzko spolupracujú s regulačnými orgánmi už od počiatočných fáz vývoja. Tento prístup nám umožňuje integrovať regulačné požiadavky priamo do procesu inovácie. Významným faktorom je naša spolupráca s výskumnými inštitúciami a účasť v medzinárodných inovačných programoch, kde môžeme testovať nové technológie v kontrolovanom prostredí.

Ako vaše vojenské pozadie ovplyvňuje prístup k vývoju kybernetických bezpečnostných riešení?

MA: Vojenské pozadie nám poskytlo jedinečnú perspektívu v oblasti kybernetickej bezpečnosti, ktorá sa premieta do vývoja našich riešení. Chápeme, že v reálnych operačných podmienkach je kritická technická dokonalosť systému, ako aj jeho odolnosť, spoľahlivosť a schopnosť fungovať pod extrémnym tlakom. Tento prístup sa prejavuje v dôraze na robustnosť našich riešení, implementáciu redundantných systémov a schopnosť rýchlej adaptácie na meniace sa hrozby. Zároveň aplikujeme princípy vojenskej stratégie v oblasti kybernetickej obrany vrátane vrstvenej ochrany, aktívnej detekcie hrozieb a schopnosti rýchlej reakcie na incidenty.

Ako riešite interoperabilitu vašich bezpečnostných systémov s existujúcimi vojenskými a civilnými infraštruktúrami?

MA: Interoperabilita predstavuje kľúčový aspekt našich riešení, keďže moderné obranné systémy musia efektívne fungovať v komplexnom prostredí zahŕňajúcom rôzne platformy a štandardy. Náš prístup je založený na implementácii medzinárodných štandardov NATO a EÚ, pričom kladieme dôraz na modulárnu architektúru našich systémov. To umožňuje jednoduchú integráciu s existujúcimi infraštruktúrami a adaptáciu na špecifické požiadavky jednotlivých zákazníkov. Významnou súčasťou je aj vývoj špecializovaných rozhraní a protokolov, ktoré zabezpečujú bezpečnú komunikáciu medzi rôznymi systémami pri zachovaní najvyšších bezpečnostných štandardov.

Foto – archív Decent Cybersecurity

NM2500411/1