Výzkum a nové technologie v kybernetické a informační bezpečnosti

Nová platforma pro spolupráci v ochraně systémů strojového učení

(22. 10. 2020, microsoft.com) Společnost Microsoft ve spolupráci s řadou dalších organizací jako MITRE, IBM nebo NVIDIA představila novou otevřenou platformu, která má pomoci analytikům kybernetické bezpečnosti při detekci, předcházení a reakci na útoky proti systémům založeným na strojovém učení. Nová platforma nese název Adversarial ML Threat Matrix a je dostupná na GitHub. Jejím cílem má být především organizace a sběr různých technik využívaných útočníky.

Komentář: S rozvojem využívání technologií umělé inteligence a strojového učení roste i nebezpečí jejich zneužití. U strojového učení však nedochází k útokům skrze specifické slabiny softwaru nebo hardwaru. Tyto útoky se zaměřují na využívaní slabin algoritmů strojového učení. U těch se útočníci snaží dané algoritmy „ošálit“ pomocí speciálně upravených datasetů a tím dosáhnout nesprávných rozhodnutí a potažmo i ohrožení celého napadeného systému. Vytváření podobných platforem je dobrým zdrojem pro rozvoj kybernetické bezpečnosti. V případě strojového učení je o to zásadnější, že v dohledné době lze dle některých organizací očekávat výrazný nárůst právě tohoto typu útoků. Například dle Gartner report bude do roku 2022 až 30 % kybernetických útoků mířit na systémy strojového učení.

Snížení nedostatku odborníků na kyberbezpečnost?

(11. 11. 2020; scmagazine.com) Dle průzkumu od společnost International Information System Security Certification Consortium došlo v tomto roce ke snížení počtu chybějících odborníků na kybernetickou bezpečnost. V minulém roce chybělo globálně téměř 4 miliony odborníků na kybernetickou bezpečnost. V letošním roce se tento nedostatek snížil na 3,1 milionu. Podobná data ukazují i další společnosti. Nedostatek odborníků na kybernetickou bezpečnost však zůstává stále klíčovým tématem pro zajišťování kybernetické bezpečnosti organizací. Najít vhodného kandidáta na pozici v oblasti kybernetické bezpečnosti je dle organizace CyberSeek v průměru o 21 % časově náročnější než najít vhodného kandidáta na jiné oblasti v IT. Jednou z nejžádanějších pozic, kterou mají organizace problém zaplnit je analytik kybernetické bezpečnosti.

Komentář: V ČR již v minulém roce byly sektory, které měly výrazné potíže s obsazováním volných pozic. Častým problémem bývá podceňování důležitosti kybernetické bezpečnost ze stran vedení organizací, které se potom odráží i v nedostatečně lákavých platových podmínkách pro odborníky. Nedostatek odborníků zůstane velmi pravděpodobně přetrvávajícím problémem v ČR i v následujících letech a může vést k vyššímu počtu úspěšných kybernetických útoků.

Vysokoškolské studium a příprava odborníků pro kvantovou éru

(12. 11. 2020, sciencedaily.com) Skupina tří výzkumníků provedla rozhovory se dvaceti manažery různých společností, které se zabývají vývojem kvantových technologií. Jejich cílem bylo získat představu jaké znalosti by měl mít ideální kandidát pro odbornou práci v oblasti kvantových počítačů. Na základě rozhovorů došli k závěru, že v současné době by univerzity měly poskytovat alespoň základní multidisciplinární kurzy, které by studenty seznámili s kvantovými počítači z pohledu informatiky, fyziky a techniky. Zdůrazňují, že takové kurzy by měly být nabízeny širokému spektru studentů, protože kvantové počítače ovlivní do budoucna výrazný počet vědních disciplín. Jedním z výstupů studie je i návrh sylabů dvou vstupních kurzů do oboru a potažmo i jedné celé studijní specializace.

Komentář: Kvantové počítače představují velkou výzvu budoucnosti. Jejich výrazné nasazení sice nemůžeme očekávat během několika málo let, ale je vhodné, aby budoucí odborníci na tuto oblast byly vychováváni již dnes. Kvantové počítače totiž představují do budoucna i velkou výzvu pro zajištění kybernetické bezpečnosti. Podobné výzkumy, které mapují, jaké znalosti tito odborníci budou potřebovat jsou tak již v této době více než na místě.

PETR MARTINEK; p.martinek@nukib.cz

Oddělení výzkumu a evropské spolupráce, NÚKIB