AI mění pravidla hry: Kyberútoky jsou sofistikovanější než kdy dřív

15.11.2024 - | PROTEXT

Společnost Kaspersky ve svojí nejnovější studii nazvané Cyber defense & AI: Are you ready to protect your organization? (Kybernetická obrana a umělá inteligence: Jste připraveni chránit svoji organizaci?) shromáždila názory odborníků, kteří se zabývají bezpečností IT a ochranou dat v mnoha různých firmách, ohledně nových potíží při obraně před kybernetickými útoky zahrnujícími použití umělé inteligence. Většina účastníků průzkumu (76 %) uvedla, že počet kybernetických útoků na jejich organizace v posledních 12 měsících vzrostl, a 46 % se zároveň domnívá, že většina těchto kybernetických útoků byla vedena pomocí AI.

Využití AI kyberzločinci je vážným problémem pro 72 % respondentů. Tlak této výzvy nutí firmy, aby přehodnotily svoje strategie kybernetické bezpečnosti a hledaly proaktivní a komplexní řešení. Za nejdůležitější faktory pro účinnější obranu proti hrozbám podporovaným AI považují pravidelná školení k rozvíjení interních odborných znalostí (92 %), vysoce kvalifikovaný personál (91 %) a využívání příslušných externích odborných znalostí v oblasti kybernetické bezpečnosti (90 %). Uvědomují si také, že je důležité mít dostatek zaměstnanců v IT týmech (80 %) a používat kvalitní bezpečnostní řešení třetích stran (86 %).

Navzdory rostoucímu povědomí o problémech spojených s AI odhaluje studie znepokojující nedostatky v připravenosti mnoha firem. Více než polovině dotazovaných organizací chybí klíčové zdroje potřebné k řešení těchto sofistikovaných hrozeb – 57 % nemá přístup k potřebným externím odborným znalostem v oblasti kybernetické bezpečnosti, 54 % uvádí, že jejich IT týmy nejsou dostatečně početné, 49 % chybí vysoce kvalifikovaní pracovníci a 52 % se málo věnuje pravidelným školením. Kromě toho si 53 % respondentů myslí, že jejich bezpečnostní opatření neodpovídají aktuální složité situaci, což je vystavuje potenciálním zranitelnostem. Většina respondentů sice tvrdí, že ví, jak tento nedostatek zdrojů řešit, faktem však zůstává, že je zatím nemají.

„Situace v oblasti kyberbezpečnosti čelí narůstajícím hrozbám, přičemž ransomware opět nabývá na síle. AI sice přináší nové možnosti, například při vytváření přesvědčivých phishingových zpráv, hlavní hrozbou jsou však rostoucí organizovanost a inovace kyberzločinců. Ti nabízejí nástroje usnadňující útoky i méně zkušeným hackerům. Firmy by měly zabezpečit IT infrastrukturu robustními vícevrstvými řešeními a využívat ekosystémy XDR s expertní podporou. Klíčovou obranou zůstávají také školení zaměstnanců o základech kybernetické bezpečnosti a bezpečném využívání AI,“ říká **Oleg Gorobets**, odborník na ochranu podnikové infrastruktury ve společnosti Kaspersky.

Celá zpráva s dalšími zjištěními je k dispozici zde.

K ochraně firem před kybernetickými hrozbami s podporou AI společnost Kaspersky doporučuje:

Zajistěte, aby každá úroveň a součást vaší IT sítě byly chráněny spolehlivými vícevrstvými ochrannými řešeními. Všechna řešení společnosti Kaspersky, počínaje produktovou řadou Kaspersky Next, obsahují velmi pokročilé technologie umělé inteligence určené k automatickému blokování nových hrozeb. Její vícevrstvá ochrana zahrnuje nejen detekci a blokování hrozeb, ale také zmenšování prostoru pro útoky prostřednictvím dalších opatření pro posílení bezpečnosti, jako je kontrola aplikací, kontrola webu a správa zranitelností a záplat. Ujistěte se, že tato bezpečnostní

řešení podporují vzájemnou kompatibilitu, aby váš tým měl jednotný dohled nad firemním zabezpečením. Zde vstupuje do hry XDR – implementace organického ekosystému XDR od jednoho dodavatele je vždy lepší volbou, a proto se přirozeně nabízí Kaspersky Next XDR Expert. Získejte nejlepší odborné znalosti v oblasti kybernetické bezpečnosti, abyste dokázali odhalit a potlačit komplexní hrozby, které jsou stále sofistikovanější, protože nástroje AI pomáhají útočníkům provádět přesněji cílené útoky. Pokud vám chybí interní odborné znalosti, můžete využít službu Kaspersky Managed Detection & Response a online nebo živá školení Kaspersky Cybersecurity, které posílí vaše interní dovednosti. Zapojte svoje zaměstnance v kanceláři jako další vrstvu obrany pomocí platformy Kaspersky Automated Security Awareness Platform, která jim vštípí zásady bezpečného chování v kyberprostoru. Zahrnuje specializované sekce věnované hrozbám s podporou AI a bezpečnému používání nástrojů AI, které pomáhají předcházet rizikům spojeným s rostoucím rozšířením těchto hrozeb.

http://www.ceskenoviny.cz/tiskove/zpravy/ai-meni-pravidla-hry-kyberutoky-jsou-sofistikovanejsi-nez-kdy-driv/2596142