**Uczenie maszynowe może ocalić Twoją firmę przed wyciekiem danych.**

**Przedsiębiorstwa wciąż zmagają się z atakami ransomware, phishingiem, wyciekami danych oraz innymi zagrożeniami, które narażają ich bezpieczeństwo i budżet. Większość firm ma świadomość, iż potrzeba im rozwiązania, które ochroni ich infrastruktury przed złośliwym oprogramowaniem i innymi cyberzagrożeniami.**

Do roku **2022** ochrona danych i cyberterroryzm zwiększą popyt na technologie ochronne, generując wzrost na rynku cyberbezpieczeństwa na poziomie **200 miliardów** dolarów, informuje portal **marketsandmarkets.**

Rosnąca liczba agresywnych ataków na krytyczne infrastruktury i ogólny wzrost stopnia zaawansowania malware, skłoniło ekspertów bezpieczeństwa do wykorzystania algorytmów uczenia maszynowego, które mają poprawić poziom najnowszych rozwiązań chroniącymi przed cyberzagrożeniami.

Mimo tego, iż według wielu ekspertów uczenie maszynowe nie jest kompleksowym rozwiązaniem, to jeden z elementów solidnego zabezpieczenia. Konsekwencje wykorzystywania wspomnianych algorytmów mogą być na dłuższą metę rewolucyjne dla branży cyberbezpieczeństwa, mogą również zwiększyć wydajność przez automatyzację i rozwiązać kwestię incydentów, których głównym powodem był tzw. **czynnik ludzki.**

„Algorytmy uczenia maszynowego są zaprogramowane w taki sposób, aby generować dokładne przewidywania. Cały ten proces oparty jest na analizie konkretnych zestawów danych.”, wyjaśnia **Mariusz Politowicz,** inżynier techniczny Bitdefender z firmy Marken, „Aby ochrona była kompleksowa ten model ochrony musi jednak iść w parze z innymi rozwiązaniami bezpieczeństwa. Istotną kwestią jest również jakość i objętość zestawów danych, które posłużą za bazę, na której algorytm się *uczy*” – dodaje.

W sektorze cyberbezpieczeństwa uczenie maszynowe jest bardzo efektywne jeśli chodzi o ulepszanie rozwiązań chroniących przed **malware,** jednak wciąż kwestią problematyczną jest prawidłowość i precyzyjność zestawów danych oraz wyznaczenie wzoru przeprowadzanych ataków. Nie wyklucza się jednak roli człowieka, gdyż inżynierowie wciąż aktualizują wspomniane algorytmy i dokładają starań, aby zestawy danych służących za bazę, były prawidłowe i kompleksowe.

Uczenie maszynowe stało się popularne w branży cyberbezpieczeństwa ze względu na możliwości kategoryzowania danych i analizy złośliwego kodu w czasie rzeczywistym. Wszystko po to, aby zagrożenie nie przeniosło się na inne stacje. Jak do tej pory, uczenie maszynowe o wiele bardziej sprawdziło się w zaawansowanej ochronie punktów końcowych i powstrzymywaniu zagrożeń niż tradycyjna ochrona. Rozwiązanie, o którym mowa może być bardzo cenne dla ochrony sieci złożonych z urządzeń inteligentnych **(Internet of Things network)**, które w ostatnim czasie są częstym celem cyberprzestępców.