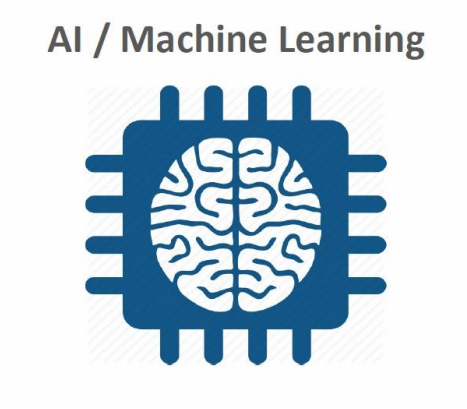

Uczenie maszynowe (*machine learning*) może zrewolucjonizować branżę cyberbezpieczeństwa, gdyż pozwala uporządkować ogromną ilość danych i szybciej wykrywać nowe zagrożenia czy kolejne warianty złośliwego oprogramowania. Rozwiązania tego typu zostały już włączone do tradycyjnych usług działających w oparciu o chmurę. W części 2 relacji z *NetEvents EMEA Press Spotlight 2018* – wybrane wypowiedzi i wnioski z paneli dyskusyjnych, które odbyły się w ramach konferencji.

źr. Fortinet

Szybkie przetwarzanie informacji i reagowanie na zagrożenia w czasie rzeczywistym jest możliwe dzięki uczeniu maszynowemu, które wykorzystuje algorytmy do analizy dużej ilości danych. Maszyna może zidentyfikować wzorce i prawidłowości oraz podejmować na tej podstawie decyzje, a wszystko przy minimalnej ingerencji człowieka.

Uczenie maszynowe wykorzystują m.in. zapory sieciowe typu WAF (*Web Application Firewalls*), które opierają się na obserwacyjnej metodzie wykrywania zagrożeń zwanej uczeniem się przez aplikację (ang. *AL – Application Learning*). AL tworzy profile sposobu korzystania z aplikacji internetowych, a wszelkie niezgodne z nimi działania klasyfikuje jako anomalię. Sztuczna inteligencja, wykorzystując uczenie maszynowe, ustala, czy jest to realne zagrożenie, a jeśli tak, WAF może rejestrować i blokować żądanie.

WYBRANE WYPOWIEDZI UCZESTNIKÓW PANELI

Rik Turner, Principal Analyst, Infrastructure Solutions, Ovum: Tylko 30-40 proc. nowych malware jest wykrywanych przez sygnatury antywirusowe, nie więcej. A szczerze mówiąc, myślę, że jest to nawet o wiele mniej. Nie ulega najmniejszej wątpliwości, że istnieje potrzeba optymalizacji działania systemów ochrony przed cyberzagrożeniami, ich agregacji, integracji, uproszczenia i automatyzacji. Wszyscy muszą połączyć siły i dołączyć z własnymi API do społeczności zwalczającej cyberprzestępczość, żeby ochrona była skuteczna.

Bardzo ważna w ramach tzw. platform play jest integracja rozwiązań różnych dostawców (na rynku dostępnych jest około 200 różnych funkcji służących do zapewniania bezpieczeństwa w cyberprzestrzeni).

Wszczepianie „inteligencji” w systemy ochrony jest niezbędne. Sztuczna inteligencja może stać się „najlepszym przyjacielem” specjalistów ds. cyberbezpieczeństwa. Machine learning pomoże w automatyzacji funkcjonowania systemów bezpieczeństwa ICT i tworzeniu systemów do predyktywnej ochrony.

MPLS nie jest martwy, ale jego wzrost będzie ograniczany przez rozwiązania SD-WAN. Dostawcy MPLS muszą sięgnąć po SD-WAN i je stosować – SD-WAN jest Netflixem na rynku WAN dla przedsiębiorstw.

Jan Guldentops, dyrektor BA Test Labs: Musimy pamiętać, że sztuczna inteligencja to narzędzie, a nie magia. Artificial intelligence to kolejne określenie, takie jak IoT czy chmura, którymi się posługujemy i ogólnie rozumiemy, ale tak naprawdę do końca zastanawiamy się, o co chodzi. I tak na przykład, antyspam wykorzystuje elementy uczenia maszynowego już od ponad 15 lat.

Roark Pollock, Ziften Technologies: Wszystko zależy od tego, co rozumie się przez sztuczną inteligencję. Na ogół używamy sztucznej inteligencji jako terminu zbiorczego, ale dziewięć razy na dziesięć mówimy o zwykłym uczeniu maszynowym (*machine learning*) i właśnie to robi większość dostawców rozwiązań zabezpieczających. Zapewniają oni obecnie w swoich produktach pewien rodzaj przetwarzanie języka naturalnego lub głębsze uczenie maszynowe.

Philip Griffiths, NetFoundry: Bezpieczeństwo jest równie ważne jak wydajność działania systemów ICT.

Scott Raynovich, Futuriom: Wszystkie decyzje dotyczące bezpieczeństwa mają charakter ekonomiczny.

Atchison Frazer, CMO, Versa Networks: Potencjalne korzyści z wprowadzania przez operatorów usług dodanych to funkcje analityczne i inteligencja wszczepiana do sieci.

Technologia oferowana przez Versa może obniżyć koszty tradycyjnych sieci MPLS poprzez integrację chmury, LTE, SD-WAN, usług bezpieczeństwa definiowanych programowo i innych sieci, ponieważ bity internetowe są o 80 proc. tańsze niż bity MPLS.

O przechodzeniu sieci rozległych WAN na poziom aplikacyjny poprzez wdrażanie rozwiązań SDN-WAN oraz APN (*Application-Specific Networks*) w poprzednim wpisie: *SD-WAN zastąpi routery*

(grafika tytułowa pochodzi z prezentacji Ovum/Informa PLC)