ZYXEL

Ogień zwalczaj ogniem. Pojedynek sztucznych inteligencji dla bezpieczeństwa sieci

Sztuczna inteligencja (z ang. Artificial Intelligence) jest jednym z wiodących tematów poruszanych podczas dyskusji nad technologiami przyszłości. Zdarza się, że wykorzystywana jest w złych celach, na przykład do włamań do sieci komputerowych. Na szczęście z tego narzędzia potrafią skutecznie korzystać także firmy produkujące urządzenia zabezpieczające.

Zdolność błyskawicznej nauki i nieustanne doskonalenie algorytmów to gwarancja szybkiego rozwoju Sztucznej Inteligencji. O ile jednak zwykle wykorzystywana jest ona do celów naukowych czy biznesowych, znajduje też zastosowania w świecie cyberprzestępczości. Cyberprzestępcy zaczynają wykorzystywać sztuczną inteligencję do tworzenia nowych zagrożeń, które są w stanie obejść zabezpieczenia konwencjonalnych zapór. Każda sieć i urządzenie będą w przyszłości narażone na nowe generacje inteligentnych wirusów, które będą nie tylko skuteczniejsze od jakichkolwiek znanych dziś zagrożeń, ale będą zdolne uczyć się w czasie rzeczywistym. Przykładowo wirus może pozostawać w stanie uśpienia przez kilka dni tylko po to, aby zostać zaklasyfikowanym jako nieszkodliwy, by następnie aktywować się. Konsekwencją działalności wirusa może być nie tylko zablokowanie komputerów w sieci, ale też kradzież dużych ilości danych osobowych i poufnych, a także wykorzystanie jednostek połączonych w sieci jako komputerów-zombie stosowanych do ataków DDoS.

Uprzedzić problem

Aby móc przeciwdziałać coraz bardziej wyrafinowanym atakom, potrzebna jest adekwatna, zaawansowana ochrona sieci. Usługa ATP (**Advanced Threat Protection**) wprowadzona przez Zyxel, w serii zapór sieciowych o tej samej nazwie, wykorzystuje sztuczną inteligencję do wykrywania i eliminowania potencjalnych zagrożeń, zanim zostaną zainstalowane i zaczną wyrządzać szkody.

Podstawowym narzędziem stosowanym w ATP jest **sandboxing**. Bada ono aktywność plików w czasie rzeczywistym, wykrywając i blokując te z nich, które są nieznane i mogą okazać się złośliwe. Usługa uruchamia je w kontrolowanym środowisku ochronnym do złudzenia przypominającym rzeczywisty system. Potencjalne zagrożenia są następnie analizowane przy użyciu sztucznej inteligencji i

najnowszych danych dostępnych w systemie ATP. Istotną częścią systemu ATP jest chmura, dzięki której wszyscy użytkownicy usługi mogą udostępniać informacje o nowych zagrożeniach niemalże w czasie rzeczywistym.

– *Hakerzy i cyberprzestępcy wykorzystują sztuczną inteligencję uczącą się jak ominąć zabezpieczenia. Naszym zadaniem w branży bezpieczeństwa sieci jest być o krok przed nimi i wykorzystywać sztuczną inteligencję do przeciwdziałania atakom* – mówi Aleksander Styś, VAR Account Manager w Zyxel Communications. – *Jest to taktyka zwalczania ognia ogniem* – dodaje.

Usługa ATP oprócz Sandboxingu oferuje też między innymi takie narzędzia jak SecuReporter służący do kompleksowej analizy danych i ich raportowania, a także narzędzia filtrujące botnety, lokalizujące zagrożenie pod względem geograficznym czy zapobiegające atakom za pośrednictwem aplikacji.

Więcej informacji znajduje się na stronie producenta.

Zyxel Communications

Zyxel Communications już od prawie 30 lat łączy ludzi koncentrując się na wdrażaniu innowacyjnych rozwiązań dla swoich klientów. Nasze możliwości adaptacji oraz innowacyjne technologie sieciowe czynią nas liderami komunikacji dla firm telekomunikacyjnych, dostawców usług, klientów biznesowych i użytkowników domowych.

- 1500+ współpracowników na całym świecie
- 100 milionów urządzeń łączących na globalną skalę
- Ponad 700,000 firm pracujących lepiej, dzięki produktom marki Zyxel
- Obecność na 150 światowych rynkach

Obecnie, Zyxel Communications tworząc sieci przyszłości, uwalnia potencjał i spełnia wymagania nowoczesnych miejsc pracy – wspierając ludzi w biurze, codziennym życiu i w czasie wolnym.

ZYXEL – twój sieciowy sojusznik

Dołącz do nas na Facebooku i LinkedIn!