Wielowarstwowa ochrona przed cyberzagrożeniami — poznaj trzy zasady

Sztuczna inteligencja to nie sen o przyszłości. Coraz częściej spotykamy się z nią na co dzień. Znajduje zastosowanie zarówno w nauce, jak i biznesie. Wykorzystują ją też producenci zabezpieczeń sieciowych, opracowując wielowarstwowe systemy ochrony, by skutecznie walczyć z coraz częstszymi cyberzagrożeniami.

Łatwo zgubić się w gąszczu możliwości oferowanych przez producentów zabezpieczeń sieciowych. Jak tego uniknąć? Warto kierować się opracowaną przez firmę Zyxel zasadą 3xZ, czyli „zablokuj, zapoznaj się, zapobiegaj". Co to w praktyce oznacza?

Zablokuj

Ochrona wielowarstwowa z domyślnej usługi bezpieczeństwa może blokować złośliwy i podejrzany ruch, zapewniając bezpieczeństwo sieci.

Pliki blokowane są za pomocą mechanizmu sandboxing czyli piaskownicy. Jeśli zapora sieciowa nie może jednoznacznie określić, czy dany plik jest całkowicie bezpieczny i nie zawiera ukrytego, szkodliwego kodu, umieszcza go w piaskownicy. To środowisko testowe, w którym uruchamiane są podejrzane pliki, a które funkcjonuje w odizolowaniu od naszego systemu. Umożliwia to separowanie zagrożenia z dala od innych urządzeń oraz plików i zabezpiecza sieć przed rozprzestrzenianiem się złośliwego oprogramowania.

Zapoznaj się

Następnie zagrożenia trzeba poznać. Mechanizm Cloud Intelligence identyfikuje wszystkie nowe zagrożenia, dodaje je do bazy danych w chmurze, uczy się ich i dzięki temu zwiększa bezpieczeństwo sieci przed kolejnymi atakami.

Chmura nigdy nie przestaje się rozwijać i ewoluować, łącząc wiele baz danych z systemem automatycznego uczenia się o zagrożeniach, a jej rosnąca inteligencja w zakresie złośliwego oprogramowania pozwala zaporom ATP na wykrywanie złośliwego oprogramowania w czasie rzeczywistym.

Zapobiegaj

Cloud Intelligence wyodrębnia najważniejsze informacje o zagrożeniach i zapewnia stałą aktualizację wszystkich zapór sieciowych ATP. Bramy uczą się od siebie nawzajem. Ta globalna synergia współdzielenia umożliwia zaporom sieciowym ATP zapobieganie ukrytym zagrożeniom.

Skąd wyciągane są wnioski? Na przykład Zyxel SecuReporter jest usługą opartą na chmurze. Została zaprojektowana do zbiorczego podglądu analiz i raportów w zakresie bezpieczeństwa cybernetycznego, a także gromadzenia i korelowania danych o zagrożeniach. Informacje o bezpieczeństwie prezentowane są w wersjach graficznych, na wykresach i w tabelach, które ułatwiają analizę danych i ich interpretację.

Czy jesteśmy przygotowani na ataki cybernetyczne?

W zaporze sieciowej ATP Zyxela wykorzystuje się uczenie maszynowe i samodzielnie rozwijającą się inteligencję chmury. Zapewnia to najwyższy poziom ochrony. Firmy, korzystające z tego rozwiązania, mogą być spokojne wiedząc, że ich systemy są monitorowane pod kątem przesyłania niebezpiecznych plików a potencjalne zagrożenia są izolowane. Dzięki temu sieci mogą pracować bez zakłóceń, zachowując bezpieczeństwo swoich danych.

– *Walka producentów zabezpieczeń z hakerami to wyścig zbrojeń. W Zyxel jesteśmy na niego przygotowani – stale rozwijamy inteligencję chmury, by móc odpowiadać na wyzwania dotyczące cyberochrony teraz i w przyszłości* – mówi Aleksander Styś, VAR Account Manager w Zyxel Communications.

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!