ZYXEL

www.Zyxel.com

Bezpieczeństwo sieciowe małych i średnich firm oparte o technologię chmury

Żyjemy w erze big data – generujemy bardzo dużo danych, które potrzebują odpowiedniej ochrony. Firmy by uchronić się przed atakami cybernetycznymi muszą podejmować natychmiastowe działania. Często w odpowiedzi na warunki, które nieustannie się zmieniają. Coraz większą popularność zyskują sieciowe rozwiązania zabezpieczające bazujące na technologii chmury, które pozwalają na bieżącą aktualizację danych o zagrożeniach i zapobieganie im.

Małe i średnie przedsiębiorstwa często napotykają na trudności związane z odpowiednią ochroną swoich sieci spowodowaną m.in. brakiem czasu czy środków na inwestycje w odpowiednią infrastrukturę sieciową. Badania pokazują, że 43% naruszeń danych dotyczy małych firm. Nie mogą one pozwolić sobie na czekanie na kolejną aktualizację zapory sieciowej lub programu antywirusowego, aby poradzić sobie z zagrożeniami.

Wybór rozwiązania SaaS (software-as-a-service) okazuje się być dla nich odpowiednią strategią. Stosowanie modelu chmury obliczeniowej SaaS to rozwiązanie, które zapewnia klientom biznesowym niezbędną elastyczność i zakres ochrony danych oraz zasobów firmowych w obliczu ataków cybernetycznych.

Umożliwia zespołom IT aktualizowanie środków bezpieczeństwa i stosowanie nowoczesnych technologii, jednocześnie powstrzymując uporczywe i stale ewoluujące narzędzia oraz sposoby ataków cybernetycznych.

Zaawansowana ochrona przed zagrożeniami

Rozwiązania SaaS, takie jak ATP i sandboxing (piaskownica), pozwalają reagować na zagrożenie w czasie rzeczywistym i automatycznie dostosowują się do postępu technologicznego w taki sam sposób, jak robi to złośliwe oprogramowanie.

Przykładem zapory sieciowej nowej generacji jest Zyxel ATP, brama wyposażona w system Zyxel Cloud Intelligence. Wykorzystuje on uczenie maszynowe do rejestrowania nieznanego zagrożenia wykrytego przez bramy ATP w chmurze i zapewniając tymże bramom codzienną aktualizację. Każde nowe zagrożenie jest przekształcane w dodatkową wiedzę dla stale rosnącego i uczącego się ekosystemu bezpieczeństwa, który cały czas dostosowuje się do nowych zaawansowanych ataków.

Natomiast Sandboxing, który jest integralnym elementem systemu, to wyodrębniona strefa w chmurze, do której trafiają nieznane, potencjalnie zagrożone pliki niewykrywalne przez standardowe mechanizmy zabezpieczeń. Tam są identyfikowane, zapewniając przy tym ochronę przed atakami typu zero-day (całkiem nowe ataki, na które producenci zabezpieczeń nie mają jeszcze sposobu). Mechanizm izoluje nieznane pliki i weryfikuje, czy są to nowe typy złośliwego oprogramowania. Sandboxing sprawdza się również jako skuteczna strategia w chmurze, ponieważ zapewnia bardziej zróżnicowany i spersonalizowany sposób konfigurowania zabezpieczeń.

Raportowanie i analityka pozwala mieć wgląd w to, co dzieje się z oprogramowaniem i ulepszać system bezpieczeństwa. Panel kontrolny zapory sieciowej Zyxel ATP oferuje przyjazne dla użytkownika infografiki ze statystykami i z listą zagrożeń.

Przejmij kontrolę

Słowem-kluczem jest „kontrola". Lepiej nie czekać na aktualizacje zapory i polegać na nich, podczas gdy zagrożenia cybernetyczne ewoluują i zmieniają taktykę.

Rozwiązania oparte na chmurze do analizy wizualnej i raportowania odciążają użytkowników, dyskretnie pracując w chmurze oraz dając ogólny widok i zestawianie danych o zagrożeniach. Personel IT może następnie wykorzystać odpowiednie statystyki i dane według własnego uznania, zanim podejmie bardziej świadome środki zapobiegawcze przeciwko wykrytym zagrożeniom.

Przyszłościowe rozwiązanie zabezpieczające

Najważniejsza decyzja dotycząca rozwiązań zabezpieczających opartych na technologii chmury dotyczy wyboru zaufanego dostawcy takich usług. Obecnie zasoby danych przechowywane w firmach – nie są tak bezpieczne jak te pod kontrolą firm trzecich, które stosują odpowiednie zabezpieczenia.

Usługi te rozwijają się nie tylko pod kątem zagrożeń, ale są i będą skalowane wraz z ciągłym udoskonaleniem i ekspansją firmy. Co więcej, SaaS zapewnia możliwości personalizacji, które eliminują problemy pochłaniające czas oraz koszty. SaaS to rozwiązanie przyszłości pracujące wydajnie i umożliwiające kompleksowe zarządzanie ryzykiem zagrożeń sieciowych – wszystko pod kontrolą zaufanego partnera.

-- *Parametry takie jak wydajność, bezpieczeństwo cybernetyczne i funkcjonowanie w przyszłości wiążą się z wyjściem z początkowej fazy rozwoju małych i średnich firm. Im większa staje się firma tym więcej generuje danych i bardziej narażona jest na ich utratę* – podkreśla Aleksander Styś, VAR Account Manager w Zyxel Communications.

Powierzenie chmurze swoich danych może być najbardziej odpowiedzialnym krokiem, jaki można podjąć, aby uchronić się przed nowymi zagrożeniami.

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!