**Zyxel Networks liderem globalnego sektora sieciowego SMB we wdrażaniu Secure by Design**

**Wzmocnienie uwierzytelnienia wieloskładnikowego, zarządzanie podatnościami i przejrzystość.**

**Zyxel Networks**, lider w dostarczaniu bezpiecznych i opartych na sztucznej inteligencji rozwiązań sieciowych w chmurze, przedstawił swoje postępy w realizacji zobowiązania **Secure by Design**. Inicjatywa Agencji Bezpieczeństwa Cybernetycznego i Infrastruktury (CISA) zachęca producentów na całym świecie do integrowania bezpieczeństwa już od początkowej fazy projektowania, promując tym samym przejrzystość i tworzenie produktów, które są domyślnie bezpieczne.

Jako jeden z pierwszych w branży zwolenników inicjatywy CISA **Secure by Design**, **Zyxel Group** była nie tylko pierwszą firmą z Tajwanu, która wzięła w niej udział. Była także jedną z pierwszych na globalnym rynku sieciowym SMB, co podkreśla jej wiodącą pozycję w proaktywnych działaniach na rzecz cyberbezpieczeństwa.



Od tamtego czasu marka **Zyxel Networks** metodycznie pracowała nad wdrożeniem celów CISA S**ecure by Design** w całym portfolio produktów dla małych i średnich przedsiębiorstw, w tym:

l **Uwierzytelnienia wieloskładnikowego (MFA):** Wszystkie urządzenia zarządzane w chmurze **Nebula**, w tym zapory sieciowe, routery, przełączniki i punkty dostępowe, obsługują MFA. Firma **Zyxel Networks** stała się pierwszym na świecie dostawcą oferującym MFA dla dostępu bezprzewodowego za pośrednictwem funkcji **Secure WiFi**. Umożliwia administratorom egzekwowanie bezpiecznego dostępu dla zdalnych użytkowników punktów dostępowych. W przypadku zapór sieciowych MFA jest również włączone zarówno dla logowania administracyjnego, jak i zdalnych użytkowników VPN, przy użyciu weryfikacji e-mailowej lub integracji z kontami Microsoft i Google.

l **Eliminacji domyślnych haseł:** Urządzenia dostarczane z fabryki są wstępnie wyposażone w losowe, unikatowe hasła, które należy zmienić podczas konfiguracji (zapewnia to lepsze bezpieczeństwo od razu po wyjęciu z pudełka). W przypadku sieci zarządzanych przez platformę chmurową **Nebula** użytkownicy są zobowiązani do utworzenia silnych haseł przy pierwszym logowaniu.

l **Redukcji całych klas podatności na ataki:** Przyjęto solidne praktyki bezpiecznego kodowania i rozwoju, w tym przestrzeganie OWASP Top 10, korzystanie ze statycznego kodu i narzędzi do analizy firmware’u (m.in. Checkmarx) oraz zaawansowanych technik (np. zautomatyzowanych testów kombinatorycznych (ACTS). **Zyxel Networks** współpracuje również z niezależnymi firmami zewnętrznymi przeprowadzającymi testy penetracyjne, aby ograniczyć “ślepe punkty” w procesie rozwoju produktów.

l **Zapewnienia terminowych poprawek zabezpieczeń:** Rekord **Zyxel Group** w zakresie terminowego łatania luk w zabezpieczeniach jest wzmocniony przez przez pełnioną funkcję **CVE Numbering Authority (CNA)** (od 2021 roku). W ciągu ostatnich 5 lat średni czas naprawy (MTTR) firmy pozostawał zgodny ze standardami branżowymi. Odzwierciedla ciągłe inwestycje w szybkie, skoordynowane mechanizmy reagowania.

l **Ustanowienia polityki ujawniania luk w zabezpieczeniach (VDP) i przejrzystości w zgłaszaniu luk:** Grupa **Zyxel** wdrożyła kompleksową politykę VDP z jasnymi wytycznymi i publicznie dostępnymi kanałami raportowania. Przejrzystość w raportowaniu i ujawnianiu informacji zapewniła jej najwyższy poziom akceptacji CNA, który do tej pory nie ma sobie równych wśród innych marek sieciowych dla średnich i małych firm.

l **Zwiększonego gromadzenia dowodów włamań:** Wszystkie produkty **Zyxel Networks Nebula** zarządzane w chmurze zapewniają teraz od 7 do 30 dni szczegółowych logów sieciowych.Informacje na temat bezpieczeństwa są dostarczane za pośrednictwem **SecuReporter**, opartej na chmurze platformy analitycznej, która oferuje scentralizowany widok aktywności sieciowej i zagrożeń. W przypadku zapór sieciowych i routerów bezpieczeństwa, dzienniki dostępu i operacyjne są przechowywane przez okres do 12 miesięcy. Umożliwia to kompleksowe audyty i reagowanie na incydenty.

*Wierzymy, że bezpieczeństwo musi być wbudowane, a nie przykręcane* - powiedział **Norbert Ogłoziński**, Country Sales Manager, **Zyxel Networks Polska**. - *Nasze zaangażowanie w* ***Secure by Design*** *pomaga nam chronić naszych klientów i partnerów w szybko zmieniającym się krajobrazie zagrożeń. Przyczynia się do zdrowszego ekosystemu IT, a przejrzystość w raportowaniu luk w zabezpieczeniach jest znakiem rozpoznawczym odpowiedzialnej, nowoczesnej praktyki bezpieczeństwa. Nasze podejście opiera się na otwartości, uczciwości i długoterminowym zaufaniu, co jest w pełni zgodne z wizją CISA i, co ważniejsze, oczekiwaniami naszych klientów*.

Więcej informacji na temat portfolio produktów **Zyxel Networks**, które uwzględniają zasady **Secure by Design**, można znaleźć na stronie [**www.zyxel.com**](http://www.zyxel.com).