Kontakt dla mediów:

email: media@parp.gov.pl

Informacja prasowa

Warszawa, 02.04.2026

Zmiana ustawy o cyberbezpieczeństwie to za mało. Polski startup chce rozwiązać problemy z niedoborem specjalistów

3 kwietnia 2026 roku wchodzi w życie nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa (UKSC), wdrażająca unijną dyrektywę NIS 2. Ma ona poprawić odporność infrastruktury krytycznej na cyberataki, których liczba stale rośnie. Wyzwaniem w Polsce jest jednak niedobór specjalistów w dziedzinie cyberbezpieczeństwa, a absolwentom kierunków informatycznych wchodzącym na rynek pracy często brakuje praktycznych umiejętności w tym obszarze. W odpowiedzi na te potrzeby firma Cyberrange wprowadza na rynek innowacyjną platformę szkoleniową z zakresu cyberbezpieczeństwa, stanowiącą pierwsze tego typu rozwiązanie w Polsce. Startup otrzymał wsparcie w ramach działania „Startup Booster Poland" z programu Fundusze Europejskie dla Nowoczesnej Gospodarki (FENG), realizowanego przez Polską Agencję Rozwoju Przedsiębiorczości (PARP).

W ostatnich miesiącach częstotliwość cyberataków na infrastrukturę osiągnęła poziomy, które plasują Polskę w ścisłej czołówce najbardziej zagrożonych pod tym względem krajów Europy. Według raportu KPMG „Barometr cyberbezpieczeństwa 2026", w 2025 roku aż 96 proc. polskich organizacji odnotowało przynajmniej jeden taki incydent, realnie zagrażający bezpieczeństwu firmy. Stanowi to kilkunastoprocentowy wzrost w ujęciu rocznym oraz najwyższy wynik w historii badania.[1]

Pozycja geopolityczna Polski sprawia, że kraj stał się jednym z głównych celów wojny hybrydowej prowadzonej w cyberprzestrzeni. Jednym z najpoważniejszych zagrożeń są ataki cyfrowe wymierzone w infrastrukturę krytyczną i przemysłową. Atakujący dążą do przejęcia kontroli nad procesami technologicznymi m.in. w fabrykach czy elektrowniach.

– Choć część ataków przypisywana jest grupom powiązanym z Rosją i Białorusią, ich rzeczywiste źródło jest często maskowane poprzez wykorzystanie serwerów VPN oraz infrastruktury rozproszonej na całym świecie. W pierwszych dniach po inwazji Rosji na Ukrainę, polskie spółki zbrojeniowe były atakowane z częstotliwością kilkudziesięciu razy na minutę. Gdyby adresy pochodzące z Rosji, Białorusi czy Chin nie były wykluczone, próby

[1] Barometr cyberbezpieczeństwa 2026

włamań liczylibyśmy nie w dziesiątkach, a w setkach – mówi **Michał Wasielewski, CEO w Cyberrange.**

Deficyt ekspertów problemem dla rynku

Rosnąca częstotliwość ataków cyfrowych sprawia, że organizacje w coraz większym stopniu potrzebują usług specjalistów ds. cyberbezpieczeństwa. Według raportu KPMG jedynie 2 proc. firm biorących udział w badaniu nie posiada w swoich strukturach osób formalnie odpowiedzialnych za ochronę przed atakami cyfrowymi.[2] Branża odnotowuje jednak lukę rynkową między liczbą ekspertów a popytem na ich usługi. Przyczynia się do tego m.in. niedostateczne przygotowanie absolwentów kierunków informatycznych w obszarze cyberbezpieczeństwa.

– Informatyka sama w sobie to za mało. Branża potrzebuje ekspertów potrafiących operować w realnych, złożonych architekturach sieciowych, a nie tylko zarządzać infrastrukturą IT. Osoba świeżo po takich studiach zwykle nie ma praktycznego doświadczenia. Wiedza z zakresu cyberbezpieczeństwa zmienia i rozwija się bardzo dynamicznie, więc nawet osoby chcące dokształcić się we własnym zakresie mogą nie mieć dostępu do najnowszych narzędzi – podkreśla **Michał Wasielewski.**

Nowoczesne podejście do cyberbezpieczeństwa

Rozwiązaniem tego problemu jest innowacyjna w skali kraju platforma **Cyberrange**. Jej głównym założeniem jest skupienie się na praktycznych aspektach bezpieczeństwa cyfrowego. Pozwala ona na rozwijanie kompetencji w bezpiecznym, kontrolowanym środowisku, odwzorowującym rzeczywiste sieci, procesy oraz scenariusze włamań i obrony.

System integruje trzy rodzaje zadań. Tryb „Red Team" umożliwia realizację pełnego cyklu ataku, ucząc kursantów logiki działań, od rekonesansu po przejęcie celu. Z kolei tryb „Blue Team" odzwierciedla realia pracy w centrach operacji bezpieczeństwa (SOC), gdzie użytkownik, wspomagany przez sztuczną inteligencję wcielającą się w rolę obrońcy, uczy się monitorowania ruchu i rozwiązywania incydentów w czasie rzeczywistym. Całość uzupełnia tryb „Guided", oferujący realne zadania realizowane krok po kroku z wykorzystaniem systemu automatycznych podpowiedzi.

Oprócz szkoleń dla kadr IT startup kładzie duży nacisk na bezpieczeństwo przemysłowe (OT), które w obecnych realiach geopolitycznych zyskuje na znaczeniu. Eksperci z Cyberrange tworzą tzw. „cyfrowych bliźniaków" sieci fabryk czy elektrowni. Dzięki temu kursanci mogą ćwiczyć wykrywanie luk w zabezpieczeniach i testować ataki w wirtualizowanym środowisku.

[2] Barometr cyberbezpieczeństwa 2026

Fundusze Europejskie wspiera polskie cyberbezpieczeństwo

Potencjał platformy został dostrzeżony przez PARP oraz Łódzką Specjalną Strefę Ekonomiczną – ŁSSE, która przyznała firmie dofinansowanie w ramach programu Fundusze Europejskie dla Nowoczesnej Gospodarki (FENG) 2021-2027, działanie „Startup Booster Poland – Spark 3.0”.

– Mam same pozytywne odczucia, jeżeli chodzi o PARP i ŁSSE. Współpracowałem już z wieloma organizacjami wspierającymi przedsiębiorców, ale jeżeli chodzi o procedurę rekrutacyjną, o wyrozumiałość czy wsparcie, nigdy jeszcze nie przebiegło to tak gładko. W ramach partnerstwa, nasza platforma została także zaprezentowana podczas łódzkiego Demo Day. Korzystając z okazji, chciałbym serdecznie podziękować Departamentowi Innowacji ŁSSE, kierowanemu przez Panią Dyrektor Magdę Kubicką, za istotny wkład w rozwój rozwiązania oraz wsparcie na kluczowych etapach projektu – mówi **Michał Wasielewski.**

Fundusze Europejskie dla Nowoczesnej Gospodarki
Rzeczpospolita Polska
Dofinansowane przez Unię Europejską
PARP Grupa PFR