Kontakt dla mediów:
Luiza Nowicka, PARP
e-mail: luiza_nowicka@parp.gov.pl
tel.: 880 524 959

Informacja prasowa
Warszawa, 14.04.2022 r.

Polskie firmy tworzą zabezpieczenia przed cyberatakami

Globalne koszty cyberprzestępczości będą rosły o 15% rocznie w ciągu najbliższych pięciu lat, osiągając do 2025 r. 10,5 bln USD rocznie, w porównaniu z 3 bln USD w 2015 r., przewiduje Cybersecurity Ventures. Wskazują też, że ponad 50% wszystkich cyberataków dotyczy małych i średnich firm, a 60% z nich wypada z działalności w ciągu sześciu miesięcy od padania ofiarą naruszenia bezpieczeństwa danych lub włamania. Polskie firmy coraz częściej zdają sobie sprawę z tego zagrożenia. W 2020 r. 95% z nich stosowało środki bezpieczeństwa ICT. W narzędzia służące zabezpieczeniu teleinformatycznemu, mogą zaopatrywać się u polskich producentów, bo nad Wisłą nie brakuje start-upów, działających w tej branży. Odnoszą sukcesy na rynku krajowym i próbują konkurować na rynkach zagranicznych. Najbardziej obiecujące projekty otrzymały dofinansowanie ze środków funduszy europejskich w ramach działań realizowanych przez Polską Agencję Rozwoju Przedsiębiorczości.

ScaleUp to jeden z programów Polskiej Agencji Rozwoju Przedsiębiorczości (PARP) skierowany do start-upów. Jego celem jest zapewnienie wsparcia eksperckiego i finansowego oraz umożliwienie nawiązania kontaktu startupom z dużymi przedsiębiorstwami, w tym ze spółkami Skarbu Państwa. Z kolei Programy Akceleracyjne PARP łączą początkujących, kreatywnych przedsiębiorców z infrastrukturą oraz doświadczeniem dużych przedsiębiorstw. Oba finansowane są z funduszy europejskich w ramach Programu Inteligentny Rozwój (PO IR) i w obu wśród dofinansowanych firm znajdziemy te, działające w branży cyberbezpieczeństwa.

– Dostrzegamy, że branża cyberbezpieczeństwa zyskuje na znaczeniu. Przygotowany przez PARP „Raport o stanie sektora małych i średnich przedsiębiorstw w Polsce", wskazuje, że w 2020 r. odsetek przedsiębiorstw stosujących środki bezpieczeństwa ICT wyniósł 95%. Z satysfakcją obserwujemy fakt, że w dziedzinie bezpieczeństwa teleinformatycznego działa coraz więcej polskich firm, proponujących innowacyjne rozwiązania. Dzięki wsparciu z funduszy europejskich mogą one rozwijać swoje technologie i nawiązywać współpracę z ważnymi partnerami. Dla polskiej gospodarki rozwój tych firm, ich rosnąca pozycja na rynku, to bardzo dobra wiadomość – podkreśla **Dariusz Budrowski**, prezes PARP.

Zabezpieczenia dla przemysłu

Wśród beneficjentów funduszy europejskich, wsparcia przyznanego w ramach umowy z PARP, jest ICsec, firma oferująca rozwiązania z zakresu cyberbezpieczeństwa infrastruktury przemysłowej (zwłaszcza w tak strategicznych sektorach jak elektroenergetyka, gazownictwo czy wodociągi), ale także tej związanej z zabezpieczeniem linii produkcyjnych i technologicznych, węzłów transportowych czy centrów danych. Rozwiązania oferowane przez ICsec, pozwalają chronić zakłady produkcyjne przed cyberatakami – zapewnić ciągłość ich działania, ochronę know-how czy zasobów.

W pierwszym etapie rozwoju, ICsec zbudowała rozwiązanie sprzętowo-softwarowe do monitorowania sieci przemysłowej pod kątem wszelkich anomalii, mogących się pojawić w tej sieci, w tym cyberataków. – Wymyśliliśmy urządzenie, które można podłączyć do wszystkich instalacji, zarówno najnowocześniejszych, jak i tych starszego typu. Dotyczy to każdej infrastruktury przemysłowej sterowanej przez sterowniki PLC, niezależnie od tego, czy jest to elektrownia, kopalnia czy wodociągi – tłumaczy **Robert Juszczyk**, prezes ICsec. Wyjaśnia, że w ramach projektów, które zostały wsparte funduszami unijnymi, firma opracowuje nowe funkcjonalności oraz nowe rozwiązania w obszarze cyberbezpieczeństwa. – W tej dziedzinie nie można stać w miejscu. W tej chwili nowoczesne sieci przemysłowe są dużo szybsze i bardzo często ich rozwój idzie w kierunku sieci bezprzewodowych jak 5G, LTE, sieci kampusowych, IIoT (Industrial Internet of Things), czyli Internetu rzeczy w przemyśle. W ramach jednego z dofinansowanych projektów przygotowujemy innowacyjne rozwiązanie, w bardzo szybkiej technologii FPGA. Będzie ono działało samodzielnie, bez konieczności korzystania z dużego oprogramowania, serwera. To będzie przełomowa, bardzo mocna oferta, która spowoduje, że będziemy gotowi na dynamiczny rozwój przemysłu 4.0, w tym również technologii 5G w sieciach przemysłowych – wyjaśnia Juszczyk.

Prezes ICSec podkreśla, że w ostatnim czasie znacznie wzrosło zainteresowanie zabezpieczeniem infrastruktury przemysłowej. Część firm odpowiadających za infrastrukturę krytyczną, została ustawowo zobowiązana do zadbania o cyberbezpieczeństwo. Jednak rozwiązań poszukują także te firmy z sektorów strategicznych, których nie obowiązuje ustawa o krajowym systemie cyberbezpieczeństwa. Do tego dochodzi zainteresowanie biznesów, które mają świadomość co do wagi cyberbezpieczeństwa i od dłuższego czasu pytają o konkretne rozwiązania. – Sytuacja geopolityczna związana z wojną na Ukrainie wymusiła wprowadzenie w cyberprzestrzeni stanu podwyższonej gotowości CHARLIE. Nakłada on konkretne wymagania – co do dużo częstszego raportowania, dyżurowania, przygotowania zasobów na atak w poszczególnych jednostkach, które podlegają pod tego typu wytyczne. Można powiedzieć, że rynek cyberbezpieczeństwa w Polsce bardzo mocno się otwiera. W tej chwili do nas, jako do producenta, wpływa bardzo wiele zapytań o informację, ofertę, konfigurację, terminy i łańcuch dostaw. Czekaliśmy na to, od lat edukowaliśmy rynek, ale dopiero teraz osoby odpowiedzialne za automatykę przemysłową rozumieją to, przed czym ich przestrzegaliśmy. Zagrożenia, na które wskazywaliśmy, w tej chwili

stały się faktem. Wkraczamy w etap, na którym mamy szansę zacząć generować znaczące przychody z działalności w branży cyberbezpieczeństwa – mówi prezes ICsec.

Dziś ICsec jest już poza fazą start-upu. Jest pierwszym polskim producentem profesjonalnych rozwiązań z zakresu bezpieczeństwa cybernetycznego w przemyśle. Firma korzysta z wielu źródeł finansowania, nie tylko ze środków unijnych. Zainwestowały w nią fundusze venture capital: EEC Magenta, w którym jednym z inwestorów jest Grupa Tauron, a także fundusz PGNiG Venture.

Innym z beneficjentów jest spółka Specfile Project. Firma proponuje rozwiązania w dziedzinie szyfrowania dokumentów i danych. – Zwiększone zainteresowanie tą tematyką zauważyliśmy w 2020 r., w pierwszych dwóch kwartałach po wybuchu pandemii. Bardzo dużo osób wzięło udział w naszych szkoleniach z zakresu szyfrowania danych, dokumentów, zabezpieczania ich na komputerze. Przeszkoliliśmy w tym czasie kilka tysięcy osób – mówi **Katarzyna Abramowicz**, prezes Specfile Project. Zwraca uwagę, że wzmożone zainteresowanie cyberbezpieczeństwem było związane z przejściem części pracowników na pracę zdalną, korzystaniem przez nich z domowych sieci i własnych komputerów. – W tej chwili ono nieco osłabło, ale o cyberbezpieczeństwie coraz więcej się mówi i pisze. Na razie firmy są w sferze edukowania się w tej dziedzinie, a nie szukania konkretnych rozwiązań, które zabezpieczyłyby firmowe dane. Świadomość jednak rośnie, a z każdym głośnym wyciekiem danych, z nakładanymi z tego powodu karami, firmy decydują się poświęcać więcej czasu i pieniędzy na cyberbezpieczeństwo – podkreśla prezes Specfile Project.

Bezpieczne pliki i cyfrowy list polecony

Specfile Project wśród produktów ma intuicyjne dla użytkowników narzędzie do szyfrowania dokumentów. Początkowo niezbędne było zainstalowanie aplikacji Specfile na komputerze, teraz jest dużo łatwiej. – Technologia poszła do przodu i nasze rozwiązanie nie wymaga już instalowania aplikacji. Wystarczy wejść na naszą stronę internetową, załadować dokument i zaszyfrować go. Następnie można go ściągnąć na swoje urządzenie i trzymać w bezpiecznej postaci. Rozszyfrowanie dokumentu wygląda analogicznie – tłumaczy Katarzyna Abramowicz.

Specfile Project w ofercie ma też usługę e-listu poleconego. – To aplikacja desktopowa. Wstawiamy w okienko treść listu, dodajemy załącznik i wysyłamy do adresata. Dostaje on powiadomienie o tym, że czeka na niego list polecony. Rejestruje się w naszym systemie, ustala swoje hasło i otrzymuje list. Osoba, która go nadała, dostaje z kolei potwierdzenie nadania i odebrania listu przez odbiorcę. Jest ono równoznaczne z dowodem nadania na poczcie, można posłużyć się nim w sądzie. Usługę e-listu poleconego mamy od czterech lat. Jest dobrze przygotowana. Dane są w pełni zaszyfrowane, a przekazywana w ten sposób korespondencja zabezpieczona – mówi Abramowicz.

Dodaje, że najmłodszym rozwiązaniem firmy jest system Sygnanet – jedyny polski szyfrowany system do przyjmowania zgłoszeń dla sygnalistów o nieprawidłowościach lub naruszeniach prawa.

Automatyzacja odpowiedzią na brak specjalistów

Antoni Omondi, prezes firmy Sagenso, która została wsparta dotacjami z funduszy europejskich, zwraca uwagę, że zapotrzebowanie na fachowców w dziedzinie cyberbezpieczeństwa rośnie, ale na rynku brakuje takich osób. – Kiedy trzy lata temu startowaliśmy jako firma, już się mówiło o tym, że specjalistów w dziedzinie cyberbezpieczeństwa będzie brakować. W tej chwili dane wskazują, że w Polsce na jednego specjalistę zajmującego się bezpieczeństwem informatycznym, przypada siedem otwartych etatów. Tylko w Europie brakuje w tej dziedzinie 350 tys. specjalistów, na świecie aż 3,5 mln. Niełatwo też pokonać barierę wejścia do tego zawodu. Trzeba mieć kompetencje technologiczne i wiedzieć jak technologię chronić – wskazuje **Antoni Omondi** i dodaje, że produkty oferowane przez firmę Sagenso są w pewnym sensie odpowiedzią na brak specjalistów. – To co nas wyróżnia na rynku to, to, że nasze narzędzia nie są przeznaczone dla informatyków czy inżynierów bezpieczeństwa, ale dla kadry zarządzającej. One automatyzują proces zarządzania bezpieczeństwem, jednak żeby z nich korzystać nie trzeba mieć specjalistycznej wiedzy. Zauważyliśmy potrzeby firm i stworzyliśmy kompletną usługę atrakcyjną cenowo i zakresowo, dzięki której nasi klienci są zabezpieczeni 24 godziny na dobę, 7 dni w tygodniu – mówi prezes Sagenso.

Podkreśla, że dla firm wchodzących na rynek, ważne jest nie tylko wsparcie finansowe w postaci dotacji, ale także możliwość nawiązywania kontaktów. – Program, w którym braliśmy udział, poza finansowaniem z PARP, łączył młode firmy – takie jak nasza – z dużymi korporacjami. W czasie wydatkowania funduszy w projekcie, pozyskaliśmy ważnego partnera technologicznego – firmę Samsung, która pomogła nam wejść na rynek, uwiarygodniła nas w oczach klientów. Zajmujemy się bezpieczeństwem, więc zaufanie to dla nas kluczowa sprawa. Nawiązaliśmy też ważną współpracę z integratorem rozwiązań technologicznych – firmą MCX. Takie partnerstwo było dla nas krokiem naprzód – zaznacza.

Konkurowanie z globalnymi graczami

Czy polskie firmy z branży cyberbezpieczeństwa mogą swobodnie konkurować na globalnym rynku? – To ogromne wyzwanie. USA, Izrael i Wielka Brytania to kolebki cyberbezpieczeństwa. W krajach tych na tę dziedzinę wydaje się ogromne środki. Rząd i instytucje publicznie aktywnie wspierają branże cyberbezpieczeństwa, nawiązują współprace z firmami, co stanowi dla ich technologii ważną weryfikację przed wejściem na rynek. My musimy konkurować z tymi firmami także na polskim rynku. Udaje się nam jednak wygrywać. Mamy klientów w Polsce, ale przygotowujemy się także do pierwszych wdrożeń za granicą – na rynkach krajów Europy Wschodniej, w Hiszpanii. Niebawem w ramach wygranej przez nas akceleracji jedziemy do Bostonu szukać partnerstwa – mówi prezes Sagenso.

Specfile Project przygotowuje się do wejścia na zagraniczne rynki. Katarzyna Abramowicz wskazuje, że w Europie jest już spora konkurencja w branży. – Wsparcie ze środków publicznych jest bardzo przydatne, bo brakuje dobrych praktyk, doświadczenia innych serwisów, co do ekspansji zagranicznej. Musimy działać na własną rękę. Jestem zdania, że instytucje, które

dysponują środkami unijnymi, wykonują w tej sprawie dobrą robotę – oferują wsparcie, pozwalają dotrzeć do podmiotów, które mogłyby być partnerami, dystrybutorami, a nawet klientami takich rozwiązań. Każda firma marzy o wyjściu poza Polskę, ale taki krok wiąże się z dużymi inwestycjami – zaznacza Abamowicz.

Historie firm wspartych przez fundusze europejskie pokazują jednak, że Polscy przedsiębiorcy z branży cyberbezpieczeństwa mogą odnosić sukcesy za granicą, a nawet przyciągać do siebie ludzi, których nazwiska są doskonale znane w Dolinie Krzemowej. Tak jest w przypadku firmy Ramp (dawniej Supozu Solutions), która działa w obszarze technologii blockchain. Pod koniec 2021 r. Ramp, firma stworzona przez Szymona Sypniewicza i Przemysława Kowalczyka, została zarejestrowana w USA przez rządową agencję – Financial Crimes Enforcement Network. Dzięki temu może działać w obszarze bezpieczeństwa płatności w 37 stanach. Firma, zgodnie z informacjami jej twórców, w 2021 r. urosła o 3000%, a do jej zarządu weszła Morgan Beller, która dla Facebooka tworzyła projekt wirtualnej waluty Libra.