Niemal co druga polska firma w ubiegłym roku padła ofiarą różnego rodzaju ataków hakerskich mających na celu kradzież danych, a nawet żądanie okupu. Polscy przedsiębiorcy sięgają więc po specjalistyczne zabezpieczenia cyfrowe napędzając rozwój rynku cybersecurity. Korzysta na tym m.in. Aegis Security, polska spółka należąca do klastra #CyberMadeInPoland, która dba o bezpieczeństwo cyfrowe przedsiębiorstw, placówek medycznych i urzędów. Spółka rusza po dodatkowe finansowanie rozwoju – chce pozyskać 1,5 mln zł, które w całości przeznaczy na dalsze skalowanie prowadzonego biznesu. A to dopiero początek – rynek rośnie tak szybko, że już teraz firma planuje w następnym kroku pozyskanie inwestora instytucjonalnego, rozszerzenie oferty produktowej, a potem wejście na NewConnect.

Rośnie liczba incydentów cyberbezpieczeństwa, czemu sprzyja utrzymująca się pandemia oraz rosyjska agresja na Ukrainę. Lawinowo rosną też obciążenia finansowe związane ze zwalczaniem konsekwencji naruszeń zabezpieczeń infrastruktury IT – wg. globalnego badania IBM „Cost of a Data Breach Report 2022”[1], przeprowadzonego w 17 krajach świata, średni koszt naruszenia w korporacjach wynosi aż 4,35 mln dolarów. To samo badanie pokazuje, że 83% badanych firm doświadczyło więcej niż jednego cyberincydentu.

Z kolei według polskiego badania firmy Sophos[2], w 2021 roku 37% polskich firm stało się celem cyberataku ransomware, czyli wymuszenia okupu za umożliwienie dostępu do danych zablokowanych za pomocą złośliwego oprogramowania, a średnia wysokość zapłaconego okupu wyniosła równowartość ponad 170 tys. dolarów. Dlatego tak ważne jest, aby na zagrożenia reagować szybciej i sprawniej, angażując w ten proces ekspertów.

– Raport Check Point Research[3] dotyczący cyberbezpieczeństwa plasuje Polskę dopiero na 27. miejscu wśród krajów europejskich, a wyprzedzają nas między innymi Białoruś, Estonia czy Czarnogóra. Jednocześnie konsekwentnie rośnie liczba ataków na kluczowe obszary działalności państwa, takie jak jednostki samorządu terytorialnego czy placówki medyczne. Od lutego br. na terenie naszego kraju obowiązuje trzeci (z czterech możliwych) stopień alarmowy CHARLIE-CRP, który dotyczy bezpieczeństwa cyberprzestrzeni, oznaczający podwyższone ryzyko ataków o charakterze terrorystycznym – mówi **Dariusz Chmielewski**, prezes zarządu Aegis Security.

Polskie programy wsparcia rozwoju cyfrowego

Mnogość ataków hackerskich i ich zatrważająca skuteczność potwierdzają, jak ważne jest wdrażanie polityk cyberbezpieczeństwa oraz współpraca ze specjalistami. W okresie pandemii wiele urzędów szybko i sprawnie przeniosło działania do sieci, jednak jednostki samorządu terytorialnego wymagają dalszego przygotowania do aktualnych wyzwań – służą temu m.in. unijne programy „Cyfrowa Gmina" oraz „Cyfrowy Powiat", które zapewniają wsparcie rozwoju cyfrowego i zwiększenie cyberbezpieczeństwa instytucji samorządowych. Z kolei szybko rosnące nakłady na ochronę zdrowia oraz programy finansowania przez NFZ zapewniające podnoszenie poziomu bezpieczeństwa systemów teleinformatycznych szpitali[4] pokazują, jak duże jest zapotrzebowanie na usługi zabezpieczeń sieci i systemów IT w placówkach medycznych.

– W Polsce mamy prawie 2500 gmin oraz ponad 25 000 podmiotów leczniczych takich jak szpitale i przychodnie finansowanych z budżetu państwa, a stan zabezpieczeń tych podmiotów oraz niewielka świadomość cyberzagrożeń wśród pracowników czynią z nich stosunkowo łatwe cele ataków w sieci w celu kradzieży danych osobowych pacjentów. Naszą ofertą chcemy wspierać zarówno jednostki samorządu terytorialnego, jak i placówki medyczne i w obu tych segmentach możemy pochwalić się stale rosnącym portfelem zamówień. Podpisujemy umowy z dużymi szpitalami i dziesiątkami gmin, ale potrzebujemy środków na pozyskiwanie najlepszych specjalistów, którzy te zamówienia będą w stanie skutecznie obsłużyć – dodał Dariusz Chmielewski.

Nakłady na cyberbezpieczeństwo

Coraz większą dojrzałość rynku cyberbezpieczeństwa oraz rosnącą świadomość luk w zabezpieczeniach potwierdzają dane raportu Juniper Research[5], według którego wydatki na cyberbezpieczeństwo w nadchodzącym czasie będą znacząco rosnąć – łączne nakłady na zabezpieczenia w tym obszarze na świecie mają do roku 2027 przekroczyć 226 mld dolarów. Także w Polsce dwucyfrowo rośnie wartość tego sektora: według raportu PMR[6] w roku 2021 łączne wydatki sięgnęły 1,9 mld zł (+10,4% rdr), a w roku 2022 prognozowane wydatki mają wynieść 2,1 mld zł (+11,3% rdr). W związku z tym szybko rozwijają się też polskie podmioty oferujące usługi cyberbezpieczeństwa.

– Błyskawicznie postępująca cyfryzacja działań człowieka praktycznie we wszystkich dziedzinach życia oznacza zwiększone zagrożenia w postaci podatności na cyberataki. Nie dziwi zatem, że inwestorzy coraz bardziej interesują się tym sektorem. Globalnie w 2021 roku inwestycje funduszy venture capital w podmioty z tej branży sięgnęły prawie 22 mld dolarów[7], co przekłada się na rozwój startupów doskonalących swoje pomysły w tym obszarze – powiedział **Łukasz Blichewicz**, prezes Grupy Assay, współwłaściciela Aegis Security. *– Rynek dla spółek takich jak Aegis Security jest ogromny, bo aż 38%[8] krajowych podmiotów nie posiada sformalizowanych zasad zarządzania cyberbezpieczeństwem w firmie. Aktualna sytuacja geopolityczna i związane z tym coraz częstsze ataki hackerskie z pewnością przekładać się będą na zwiększone zapotrzebowanie w tym zakresie* – dodał Łukasz Blichewicz.

Działająca od 2017 roku spółka Aegis Security oferuje kompleksowe rozwiązania IT dla biznesu, audyty bezpieczeństwa, testy penetracyjne i socjotechniczne, doradztwo oraz szkolenia z zakresu cyberbezpieczeństwa, jak również przygotowanie do certyfikacji systemów zarządzania oraz usługi w zakresie ochrony danych osobowych. Jest członkiem klastra #CyberMadeInPoland, którego celem jest kształtowanie i rozwój bezpiecznej cyberprzestrzeni w Polsce. Planowane na początek października pozyskanie 1,5 mln zł, pozwoli spółce przyspieszyć skalowanie biznesu. By sprostać kolejnym zleceniom – głównie ze strony jednostek samorządu terytorialnego i podmiotów leczniczych – firma zatrudni kolejnych wysokiej klasy ekspertów specjalizujących się w budowie, wdrożeniach i integracji systemów cyberbezpieczeństwa.

To wyjątkowa okazja dla inwestorów prywatnych, bo w kolejnym kroku – na początku przyszłego roku Aegis Security sięgnie po finansowanie od inwestora instytucjonalnego, a pod koniec 2023 roku spółka planuje IPO na GPW – na rynku NewConnect.

Fundusze europejskie i polskie

W 2016 roku Unia Europejska uchwaliła dyrektywę NIS (Network and Information Systems), która zobowiązała państwa członkowskie do wprowadzenia odpowiednich środków i mechanizmów do zapewnienia bezpieczeństwa cyfrowego sieci i systemów informatycznych. W Polsce dyrektywa została wprowadzona ustawą o krajowym systemie cyberbezpieczeństwa. Obecnie trwają prace nad wdrożeniem nowelizacji dyrektywy (NIS2), która zaostrza przepisy dotyczące cyberbezpieczeństwa, dążąc do zwiększenia odporności podmiotów świadczących usługi kluczowe.

Jednocześnie rusza pilotażowy Fundusz Reagowania Kryzysowego na rzecz Cyberbezpieczeństwa ENISA – Agencji UE ds. Cyberbezpieczeństwa. Każde z państw członkowskich może ubiegać się o maksymalną kwotę dofinansowania 500 tys. euro na wzmocnienie i utrzymanie poziomu cyberbezpieczeństwa swojego kraju. W Polsce dodatkowo z końcem ub. roku powołany został Fundusz Cyberbezpieczeństwa, będący mechanizmem zapewniającym finansowanie inwestycji w sprzęt i oprogramowanie oraz pozyskanie i rozwój ekspertów w tej dziedzinie. Budowa skutecznych systemów zabezpieczeń wymaga wysokiej klasy specjalistów, stąd konieczność dalszych inwestycji w ten obszar.

[1]https://www.ibm.com/security/data-breach
[2]https://www.computerworld.pl/sophos-ransomware
[3]Raport Threat Index firmy Check Point Software, lipiec 2021 r.
[4]
https://www.nfz.gov.pl/aktualnosci/aktualnosci-centrali/wsparcie-cyberbezpieczenstwa-w-placowkach-medycznych,8211.html
[5]https://www.juniperresearch.com/researchstore/key-vertical-markets/cybersecurity-research-report
[6]https://mypmr.pro/products/rynek-cyberbezpieczenstwa-w-polsce-2021
[7]https://news.crunchbase.com/venture/cybersecurity-venture-funding-2021-record/
[8]
https://assets.kpmg/content/dam/kpmg/pl/pdf/2022/06/pl-KPMG-i-Microsoft-Monitor-Transformacji-Cyfrowej-Biznesu-2022.pdf

Aegis Security *to działający od 2017 roku zespół ekspertów, specjalizujący się we wdrożeniach, budowie i integracji systemów bezpieczeństwa oraz wsparciu organizacji w zakresie cyberbezpieczeństwa i compliance. Kompleksowe rozwiązania IT Security dla biznesu obejmują audyty bezpieczeństwa, testy penetracyjne i socjotechniczne, doradztwo oraz szkolenia z zakresu cyberbezpieczeństwa, jak również przygotowanie do certyfikacji systemów zarządzania oraz usługi w zakresie ochrony danych osobowych. Kluczowe sektory rynku obsługiwane przez Aegis Security obejmują branżę medyczną, administrację publiczną, sektor finansowy oraz hotelarski. Firma jest członkiem Klastra #CyberMadeInPoland, zrzeszającego firmy i organizacje z terenu całego kraju zajmujące się cyberbezpieczeństwem w Polsce oraz Mazowieckiego Klastra ICT, jednego z Krajowych Klastrów Kluczowych (KKK) w Polsce, którego misją jest wzrost przedsiębiorczości i konkurencyjności małych i średnich przedsiębiorców.*
Więcej informacji: aegissecurity.pl

***
Grupa Assay *to niezależny fundusz inwestycyjny z wieloletnim doświadczeniem w obszarze venture capital. Działa w pionierskim na krajowym rynku modelu biznesowym, opartym na akwizycji i współprowadzeniu firm, realnie angażując się w budowanie sukcesów spółek ze swojego portfela. Assay stawia na współpracę opartą o wymianę wzajemnych doświadczeń i kompetencji funduszu, inwestora oraz pomysłodawcy projektu inwestycyjnego. Zapewnia spółkom długoterminowy rozwój, jednocześnie minimalizując ryzyko inwestycyjne. Assay Management jest wpisany do rejestru Zarządzających Alternatywnymi Spółkami Inwestycyjnymi (ASI) prowadzonego przez Komisję Nadzoru Finansowego, co oznacza, że spełnia wymogi pełnej transparentności oraz najwyższe standardy obsługi i oferuje wysoki poziom bezpieczeństwa.*
Więcej informacji: www.assay.pl

Grupa Assay
press box