INSTYTUT KOŚCIUSZKI | BRIEF PROGRAMOWY | LIPIEC 2020
ISSN 1689-9873

CYBERBEZPIECZEŃSTWO PRZEMYSŁU – POLSKIE SZANSE, INWESTYCJE, INNOWACJE

Robert Siudak – Dyrektor Niewykonawczy, Instytut Kościuszki

Cyberbezpieczeństwo przestaje być wyzwaniem jedynie dla działów IT – staje się kluczowym elementem planowania procesów biznesowych w coraz większej ilości branż. Polskie przedsiębiorstwa zaczynają dotkliwie zdawać sobie sprawę z zagrożeń jakie niesie nieodpowiednie przechowywanie danych, implementowanie procesów czy projektowanie infrastruktury. Tworzy to rynek na produkty oraz usługi, które są w stanie wesprzeć bezpieczną transformację cyfrową firm.

Globalna roczna wartość rynku cyberbezpieczeństwa szacowana była w roku 2019 na ponad 110 miliardów dolarów[1]. Co ważne, niezależnie od przyjętej metodologii, zarówno bazując na danych z lat 2010-2020, jak i w ramach predykcji do roku 2027, skumulowany roczny wskaźnik wzrostu (ang. *Compound Annual Growth Rate*, CAGR) utrzymuje się na poziomie powyżej 10%, sięgając w niektórych opracowaniach nawet 14,5%[2]. Według badań, za tak dynamiczny wzrost odpowiadać będą w największej mierze dwa nowe segmenty odbiorców – firmy przemysłowe oraz małe i średnie przedsiębiorstwa. W obydwu wypadkach fakt ten stanowi wynik aktualnych trendów dotyczących dynamicznej transformacji cyfrowej MŚP, a także realizacji idei Przemysłu 4.0.

>110 000 000 0000 $

Wyniosła wartość globalnego rynku cyberbezpieczeństwa w 2019 roku.

Rozwiązania i technologie, które odpowiedać będą za znaczny wrost rynku w kolejnych latach to przede wszystkim zabezpieczenia systemów i sieci rozproszonych. Mowa w tym wypadku przede wszystkim o Internecie Rzeczy (ang. *Internet of Things*, IoT) zarówno przemysłowym, jak i tym wykorzystywanym w systemach inteligentnego miasta (ang. *Smart City*). Technologie mgły obliczeniowej (ang. *fog computing*), sieć mesz (ang. *wireless mesh network*), czy szeroko rozumiany *edge computing*, we współpracy z chmurą obliczeniową (ang. *cloud computing*) już teraz wymuszają wypracowywanie nowej logiki zabezpieczeń, w której nie istnieje w praktyce brzeg, granica sieci firmowej. Podobnie, w wypadku klasycznej pracy biurowej, segment umożliwiający bezpieczne wdrożenie

1 W zależności od przyjętej metodologii wartość ta sięgała odpowiednio: 112 miliardów w wypadku Fortune Business Insights, *Cyber Security Market Size, Share & Industry Analysis (...) 2020-2027*, 2019, https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165; 132 miliardy w wypadku Research and Market, *Global Cybersecurity Market – Forecasts from 2019 to 2024*, 2019, https://www.businesswire.com/news/home/20191122005417/en/Global-Cybersecurity-Market-Forecasts-2019-2024---Market; 161 miliardów w wypadku Mordor Intelligence, *Cybersecurity Market – Growth, Trends, And Forecast (2020 – 2025)*, 2019, https://www.mordorintelligence.com/industry-reports/cyber-security-market.

2 Mordor Intelligence, *Cybersecurity (...)*, *op.cit.*.

rozwiązań typu Przynieś Swoje Własne Urządzenie (ang. *Bring Your Own Device*, BYOD) stanowi jedną z najszybciej rozwijających się kategorii rozwiązań. Wykładniczo zwiększa się zatem nie tylko ilość ruchu sieciowego, ale także urządzeń aktywnych w obszarach, które należy zabezpieczyć. Odpowiedzią rynku cyberbezpieczeństwa na wyzwania związane z analityką i predykcją w tak skomplikowanym środowisku stanowi coraz szersze wykorzystanie sztucznej inteligencji, szczególnie w postaci uczenia maszynowego i sieci neuronowych.

CYBERBEZPIECZEŃSTWO PRZEMYSŁU 4.0 – POLSKA SZANSA

Rynek cyberbezpieczeństwa zwiększył się ponad trzydziestokrotnie w przeciągu ostatnich 14 lat, niezmiennie stanowiąc w tym okresie jedną z najszybciej rozwijających się gałęzi branży IT[3]. Inwestorzy prywatni, ale też korporacje i rządy, które postawiły na ten właśnie sektor w ramach swoich strategii rozwojowych i inwestycyjnych już teraz notują znaczne przewagi konkurencyjne na globalnym rynku – np. Izrael, Estonia, Wielka Brytania. Kolejny ważny krok dla tego rynku wciąż przed nami. W kontekście nadchodzącej fali transformacji cyfrowej, wielu globalnych graczy już teraz inwestuje znaczne środki, aby trafić w odpowiednim czasie z odpowiednią ofertą na rynek cyberbezpieczeństwa. Przykładem może być tutaj Microsoft, który w czerwcu 2020, za ponad 150 milionów dolarów wykupił izraelski startup CyberX oferujący rozwiązania dla bezpieczeństwa IoT/OT[4].

30x

Zwiększył się globalny rynek cyberbezpieczeństwa w ostatnich 14 latach.

Z perspektywy kraju takiego jak Polska, kluczowe jest, aby odpowiednio wykorzystać zasoby kapitału ludzkiego oraz funduszy prywatnych i publicznych, aby nie przegapić szans jakie niesie otwarcie nowych segmentów rynku cyberbezpieczeństwa. Biorąc pod uwagę rozbudowany system edukacji inżynierskiej m.in. w ramach sieci politechnik, ale także światowej klasy programistów budujących od ponad dwóch dekad produkty zarówno dla gigantów IT, software house-ów jak i polskich start-upów, inwestycje w gałąź rozwiązań z zakresu bezpieczeństwa przemysłu 4.0 powinny stanowić świadomą decyzję decydentów w Polsce. Praca nie rozpoczyna się w tym wypadku od zera, na rodzimym rynku już teraz pojawiają się nieliczne, ale globalnie konkurencyjne startupy takie jak ICsec czy Olympus Sky, których przykłady opisano w dalszej części opracowania.

INWESTYCJE W BEZPIECZEŃSTWO PRZEMYSŁU 4.0

Specyfika rozwiązań dla przemysłu 4.0, zakładająca budowę systemów opartych zarówno o komponenty sprzętowe (*hardware*), programistyczne (*software*), jak i szereg dedykowanych protokołów oraz standardów sprawia, że projekty te są kosztochłonne. Z jednej strony oznacza to duży margines na marżę oraz optymalizację produkcji w kontekście sprzedaży dla klientów końcowych. Z drugiej wymaga znacznych inwestycji na etapie tworzenia oraz rozwoju produktu (B+R). W tym kontekście ważni stają się partnerzy inwestycyjni umożliwiający startupom oraz innowacyjnym firmom z sektora cyberbezpieczeństwa 4.0 rozwój i skalowanie działalności, a w wielu wypadkach także dostęp do unikalnego branżowego *know-how*.

Liderzy przemysłowi coraz aktywniej rozwijają swoje działania inwestycyjne m.in. poprzez dedykowane fundusze typu Corporate Venture Capital (CVC). Globalnymi przykładami mogą być Shell Venture czy Chevron Technology Ventures. Drugi z nich ulokował kapitał m.in. w startupie Mission Secure Inc., zabezpieczającym infrastrukturę OT oraz systemy sterowania przemysłowego (ang. *Industrial Control Systems*, ICS)[5]. W Polsce dedykowane platformy inwestycyjne tworzone są przy współpracy największych spółek przemysłowych z jednostkami publicznymi, w szczególności Polskim Funduszem Rozwoju (PFR) oraz Narodowym Centrum Badań i Rozwoju (NCBiR):

Nazwa funduszu	Wartość funduszu	Twórcy
EEC Magenta	210 mln zł	Tauron Polska Energia, PFR, NCBiR
SpeedUp Energy Innovation	100 mln zł	Polska Grupa Energetyczna – PGE Ventures, PFR, NCBiR, Grupa SpeedUp
PGNiG Ventures	100 mln zł	Polskie Górnictwo Naftowe i Gazownictwo

3 Prime Index, *Cybersecurity Industry Overview*, 2019, https://etfmg.com/wp-content/uploads/2019/03/26-Prime-Indexes-CyberSecurity-Industry-Review-17102018.pdf

4 TechCrunch, Microsoft confirms acquisition of CyberX to boost security in its IoT business, 2020, https://techcrunch.com/2020/06/22/microsoft-confirms-acquisition-of-cyberx-to-boost-security-in-its-iot-business/

5 Business Wire, Mission Secure, Inc. Announces Series A Venture Financing, 2018, https://www.businesswire.com/news/home/20181010005693/en/Mission-Secure-Announces-Series-Venture-Financing

Ponadto szereg firm przemysłowych z rodzimego rynku zaczyna prowadzić aktywne działania na rzecz wspierania implementacji innowacyjnych rozwiązań w ich ekosystemach, a także szerzej w ich branży. Dobrym przykładem jest sektor chemiczny, w którym to Grupa Ciech uruchomiła spółkę Ciech R&D koordynującą m.in. współpracę ze startupami, z kolei Grupa Azoty program akceleracyjny Idea4Azoty.

Podsumowując, coraz większa liczba liderów przemysłowych zaczyna uświadamiać sobie, że w dobie transformacji cyfrowej gospodarek ich branżę także czekają daleko idące zmiany. Automatyzacja oraz optymalizacja procesów wytwórczych stworzy wiele szans, ale także szereg wyzwań z zakresu bezpieczeństwa sieci przemysłowych. Jedną z kluczowych strategii staje się w tym kontekście inwestycja we współpracę z innowacyjnymi spółkami technologicznymi, wpisująca się nie tylko bezpośrednio w cele rynkowe przedsiębiorstwa, ale także stanowiąca formę dywersyfikacji portfela spółki.

410 000 000 zł

Planują łącznie zainwestować trzy fundusze CVC stworzone odpowiednio przez Tauron, PGE i PGNiG.

CYBERBEZPIECZEŃSTWO PRZEMYSŁU 4.0 MADE IN POLAND

Polski rynek produktów cyberbezpieczeństwa to wciąż dość młoda branża, szczególnie w zestawieniu z wieloletnią obecnością rozbudowanej oferty usługowej oraz integratorskiej na lokalnym rynku. Segment rozwiązań dla przemysłu 4.0 stanowi jeszcze węższe grono, ze względu na dużą barierę wejścia zarówno w zakresie doświadczenia kadry jak i nakładów finansowych na rzecz odpowiedniego zaplecza B+R. Potwierdza to przykład zainicjowanej przez Instytut Kościuszki grupy roboczej #CyberMadeinPoland, która zrzesza ponad 30 firm z polskiej branży ITSec. Celem grupy jest edukacja rynku w zakresie wyzwań związanych z bezpieczeństwem cyfrowym, wsparcie eksportu innowacyjnych polskich technologii na rynek globalny a także współpraca publiczno-prywatna na rzecz zwiększenia inwestycji na rynek cyberbezpieczeństwa. Aby przybliżyć specyfikę rodzimych rozwiązań dla cyberbezpieczeństwa przemysłowego poniżej przedstawiono trzy studia przypadku innowacyjnych polskich startupów oraz MŚP.

ICsec

ICsec jest polskim producentem rozwiązań z zakresu cyberbezpieczeństwa (w tym rozwiązań klasy IDS – ang. *intrusion detection system*) do monitoringu sieci OT. Dzięki wieloletnim badaniom ICsec zaprojektował i przetestował innowacyjny system SCADVANCE XP, który jest dedykowany nie tylko do wykrywania anomalii, w tym cyberataków, ale również wypełnia obowiązki wynikające ze zmieniających się przepisów prawa. Własny rozbudowany program B+R, zespół doświadczonych inżynierów, a także pozyskanie kilku milionów złotych z funduszy europejskich umożliwiło ICsec nawiązanie współpracy w zakresie inwestycyjnym z EEC Magenta.

ICsec skupia się na podnoszeniu poziomu cyberbezpieczeństwa w sieciach przemysłowych oraz środowiskach systemów SCADA przedsiębiorstw z sektora infrastruktury krytycznej, usług kluczowych, a także pozostałych zakładów przemysłowych. W tym celu rozwiązanie SCADVANCE XP prowadzi monitoring sieci automatyki przemysłowej (OT) oraz wykrywa potencjalne zagrożenia i anomalie w ruchu pomiędzy urządzeniami tej sieci. System opiera się na wykrywaniu mało prawdopodobnych lub niepożądanych zdarzeń, a w wypadku ich wykrycia informuje o nich użytkownika, wskazując miejsce wystąpienia, cel ataku i prawdopodobną przyczynę. Jest to możliwe dzięki współpracy rozwiązania zarówno z warstwą *hardware*, jak i *software* w sieci użytkownika, a także zastosowaniu analizy danych typu *Big Data* oraz algorytmów uczenia maszynowego. Przykładowe wdrożenie tak skonstruowanego systemu w jednej z elektrociepłowni pozwoliło na:

- stworzenie i wygenerowanie mapy całej monitorowanej sieci,
- zoptymalizowanie konfiguracji odnalezionych i zmapowanych urządzeń,
- możliwość wcześniejszego reagowanie na wykryte anomalie w tym cyberzagrożenia,
- możliwość monitorowania zdalnej pracy zewnętrznych zespołów serwisowych.

Olympus Sky

Większość rozwiązań zabezpieczających komunikację oraz przesyłanie danych opiera się obecnie na infrastrukturze klucza publicznego wykorzystującej certyfikaty cyfrowe. Sprawdza się ona idealnie w kontekście bankowości internetowej czy wymiany e-maili, jednak okazuje się niepraktyczna w wypadku ochrony rozproszonych sieci takich np. IoT. W odpowiedzi na te wyzwania Olympus Sky rozwija autorską

technologię pozwalającą na autonomicznie zarządzanie kluczami (ang. *Autonomous Key Management*, AKM). Opiera się ona na zdecentralizowanej sieci, którą tworzą wszystkie podłączone do niej węzły końcowe, w czasie rzeczywistym komunikujące się ze sobą w celu potwierdzenia swoich poświadczeń bezpieczeństwa. Rozwiązanie wykorzystuje podobną logikę jak technologia blockchain, jednak nie jest tak skomplikowane oraz obciążające dla systemu, przez co może funkcjonować w większych sieciach łączących małe podmioty.

Technologia AKM znalazła swoje zastosowanie w platformie Zeus dedykowanej bezpieczeństwu sieci IoT. System zarządzania integralnością uwierzytelniający zarówno sprzęt, jak i oprogramowanie w całej sieci, został wdrożony m.in. w R3 Communications oraz u innych klientów na rynkach Europy Zachodniej. Firma Olympus Sky oprócz siedziby w Łodzi posiada też biuro w San Diego, a dzięki 1,8 miliona dolarów inwestycji planuje rozszerzenie działalności na kolejne sektory.

Olympus Sky

STM Solutions

STM Solutions specjalizuje się w łączeniu dwóch obszarów –IT i OT. Ich system ADS (Attack Deception System) pozwala zbierać i monitorować informacje ze świata IT ale także korelować te dane z procesami automatyki przemysłowej prowadzonej w fabryce.

ADS wykrywa anomalie bezpieczeństwa w monitorowanej infrastrukturze dzięki dostępowi w czasie rzeczywistym do różnych źródeł danych. Dedykowanym elementem ADS wspierającym ochronę infrastruktury przemysłowej jest SCADA Fault Detection System (SFDS). Umożliwia zbieranie informacji z systemów OT, korelowanie wyników z danymi IT oraz ostrzeganie o wszelkich nieprawidłowościach. Ponadto ADS pozwala użytkownikowi wdrożyć honeypoty SCADA, które imitują działanie infrastruktury przemysłowej. Jednym z przykładów wdrożenia ADS było wykorzystanie go jako systemu monitorowania wrażliwych operacji w infrastrukturze OT związanej z obsługą substancji ropopochodnych. Zadaniem produktu było monitorowanie cystern wjeżdżających na teren klienta, a także dalszych działań związanych z poszczególnymi pojazdami. Wdrożenie ADS umożliwiło automatyczną korelacją wykrytych incydentów z materiałami z nagrań z kamer przemysłowych.

STM SOLUTIONS

PRZEMYSŁOWE #CyberMadeinPoland

Wybór cyberbezpieczeństwa przemysłu 4.0 jako polskiej niszy rynkowej, a następnie rozwój programów celowych wspierających zarówno dostęp do wiedzy, funduszy, ale także pierwszych wdrożeń na krajowym rynku, powinno stanowić cel polityki rozwojowej na poziomie rządowym. Działania takie wpisałyby się w cel wychodzenia polskiej gospodarki z pułapki średniego dochodu, a jednocześnie wspierałaby cele strategiczne związane z budową cyberbezpieczeństwa infrastruktury krytycznej oraz usług kluczowych w oparciu o krajowe rozwiązania. Tworzenie krajowych standardów cyberbezpieczeństwa w wybranych segmentach rynku nieregulowanych na poziomie wspólnoty europejskiej, takich jak przemysł 4.0, stanowić powinno jeden z celów pośrednich na tej drodze.

INSTYTUT KOŚCIUSZKI

Instytut Kościuszki jest niezależnym, pozarządowym instytutem naukowo-badawczym (Think Tank) o charakterze non profit, założonym w 2000 r. Misją Instytutu Kościuszki jest działanie na rzecz społeczno-gospodarczego rozwoju i bezpieczeństwa Polski jako aktywnego członka Unii Europejskiej oraz partnera sojuszu euroatlantyckiego. Instytut Kościuszki pragnie być liderem pozytywnych przemian, tworzyć i przekazywać najlepsze rozwiązania, również na rzecz sąsiadujących krajów budujących państwo prawa, społeczeństwo obywatelskie i gospodarkę wolnorynkową.

Instytut Kościuszki jest organizatorem Europejskiego Forum Cyberbezpieczeństwa CYBERSEC oraz Polskiego Forum Cyberbezpieczeństwa – pierwszych w Polsce oraz jednych z nielicznych w Europie corocznych konferencji poświęconych strategicznym wyzwaniom płynącym z cyberprzestrzeni i dotyczących cyberbezpieczeństwa. Więcej: http://cybersecforum.eu/.

Instytut Kościuszki jest wydawcą „European Cybersecurity Journal" (ECJ). ECJ to anglojęzyczny kwartalnik ekspercki poświęcony cyberbezpieczeństwu. Zawiera artykuły wiodących analityków i liderów opinii, ekskluzywne wywiady z decydentami oraz monitoring regulacji dotyczących kluczowych aspektów związanych z cyberprzestrzenią. Więcej: http://cybersecforum.eu/czym-jest-ecj/.

Biuro w Krakowie: ul. Feldmana 4/9, 31-130 Kraków, Polska, tel.: +48 12 632 97 24,
www.ik.org.pl, e-mail: instytut@ik.org.pl

#CyberMadeInPoland

Grupa robocza #CyberMadeInPoland zrzesza polski przemysł cyberbezpieczeństwa. Jej celem jest wspieranie rozwoju sektora, a w jej skład wchodzą zarówno firmy wytwarzające produkty i usługi dla bezpieczeństwa cyfrowego, jak i organizacje otoczenia biznesu oraz jednostki badawcze zajmujące się tą tematyką. Grupa powstała z inicjatywy Instytutu Kościuszki i wspierana jest przez Związek Cyfrowa Polska.

#CyberMadeInPoland edukuje rynek w zakresie wyzwań związanych z bezpieczną transformacją cyfrową. Grupa pracuje także nad stworzeniem specjalnego funduszu celowego na ekspansję zagraniczną polskich firm z branży cyberbezpieczeństwa oraz nad przebudową oferty grantów badawczo-rozwojowych na takie, które będą realnie wspierać rozwój globalnie konkurencyjnych rozwiązań z zakresu cyberbezpieczeństwa nad Wisłą. #CyberMadeInPoland opracowuje i przedstawiane polskiemu rządowi rekomendacje dotyczące problemów i wyzwań, z jakimi zmaga się branża cyberbezpieczeństwa w Polsce.

cybermadeinpoland.pl