



Usługa w zakresie cyberbezpieczeństwa



Spis treści:

01

Mazowiecki Klaster ICT

02

Dlaczego cyberbezpieczeństwo jest kluczowe?

03

Pandemia COVID-19, jako katalizator modelu biznesowego opartego na technologiach IT.

04

Obowiązujące regulacje prawne, jako akcelerator bezpieczeństwa cybernetycznego w MŚP.

05

Usługa

06

Kontakt



Mazowiecki Klaster ICT

Mazowiecki Klaster ICT powstał z inicjatywy Instytutu Badań Rynku, Konsumpcji i Koniunktur w dniu 27 listopada 2007 roku. Koordynatorem działań Klastra jest Stowarzyszenie Rozwoju Społeczno-Gospodarczego „Wiedza”. Mazowiecki Klaster ICT jest akceleratorem innowacyjnych projektów oraz łącznikiem pomiędzy biznesem, nauką i społeczeństwem.

Obecnie, Mazowiecki Klaster ICT łączy ze sobą 9 instytutów naukowo-badawczych, 6 renomowanych polskich uczelni wyższych, 3 fundusze inwestycyjne i ponad 400 przedsiębiorstw pochodzących zarówno z sektora MŚP, jak i również dużych przedsiębiorstw oraz instytucji otoczenia biznesu.

Misją Mazowieckiego Klastra ICT jest wywarcie pozytywnego wpływu na kraj i region w obszarze ekonomicznym, gospodarczym i społecznym poprzez ciągłe tworzenie i zarządzanie innowacjami. Wykorzystujemy i optymalizujemy potencjał innowacyjności regionu i kraju oraz promujemy go na arenie międzynarodowej.

MKICT wywiera w ten sposób długotrwałe i znaczące efekty na rozwój kraju, regionu i Europy.



Dlaczego cyberbezpieczeństwo jest kluczowe?

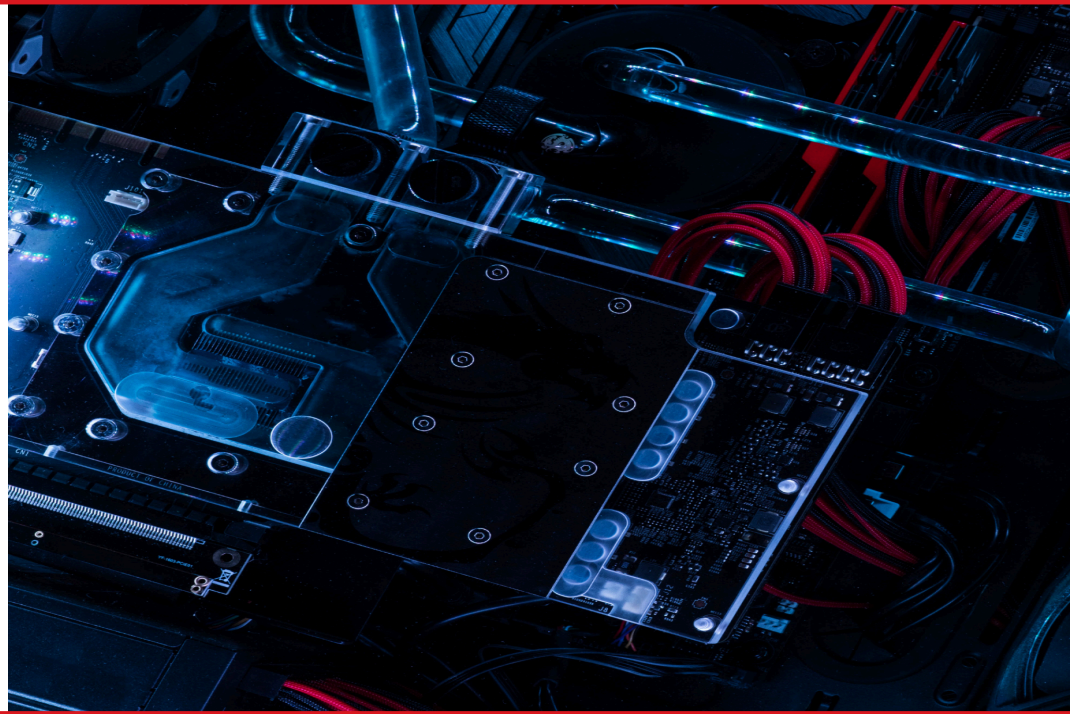
Cyberbezpieczeństwo ma istotną wartość biznesową dla odbiorców końcowych. Przechowywane cyfrowo informacje mają wartość gospodarczą, a niekiedy całe procesy związane ze świadczeniem usług i dostaw są zależne od IT. Od dostępności, wiarygodności i poufności tych danych zależy możliwość prawidłowego funkcjonowania przedsiębiorstwa.

Mnogość komponentów infrastruktury i systemów informatycznych powoduje, że kwestie cyberbezpieczeństwa są skomplikowane i specjalistyczne. Z drugiej strony liczba i różnorodność zagrożeń i ataków powoduje, że organizacje, które chcą być bezpieczne muszą być cały czas „up to date” z najnowszymi rozwiązaniami.



Pandemia COVID-19, jako katalizator modelu biznesowego opartego na technologiach IT.

Sektor MŚP musiał błyskawicznie zareagować na wpływ pandemii COVID19. Szybka reakcja na pandemię oznaczała, że większość mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (tzw. sektor MŚP) skupiła się na utrzymaniu tempa swojej działalności i podjęła wszelkie niezbędne kroki, aby zapewnić pracownikom możliwość pracy zdalnej. W niektórych przypadkach MŚP zmieniły swoje modele biznesowe, aby obsługiwać swoich klientów zdalnie przez internet. Mając to na uwadze, MŚP skupiły się przede wszystkim na zapewnieniu, że ich środowiska ICT działają w taki sposób, aby wspierać cele biznesowe. Bezpieczeństwo cybernetyczne mogło nie być głównym czynnikiem przy podejmowaniu decyzji o sposobie realizacji celów biznesowych. Skupienie się na utrzymaniu działalności biznesowej jest zrozumiałe, natomiast kluczowe środki bezpieczeństwa cybernetycznego muszą być wdrożone z należytą starannością.



Obowiązujące regulacje prawne, jako akcelerator bezpieczeństwa cybernetycznego w MSP.

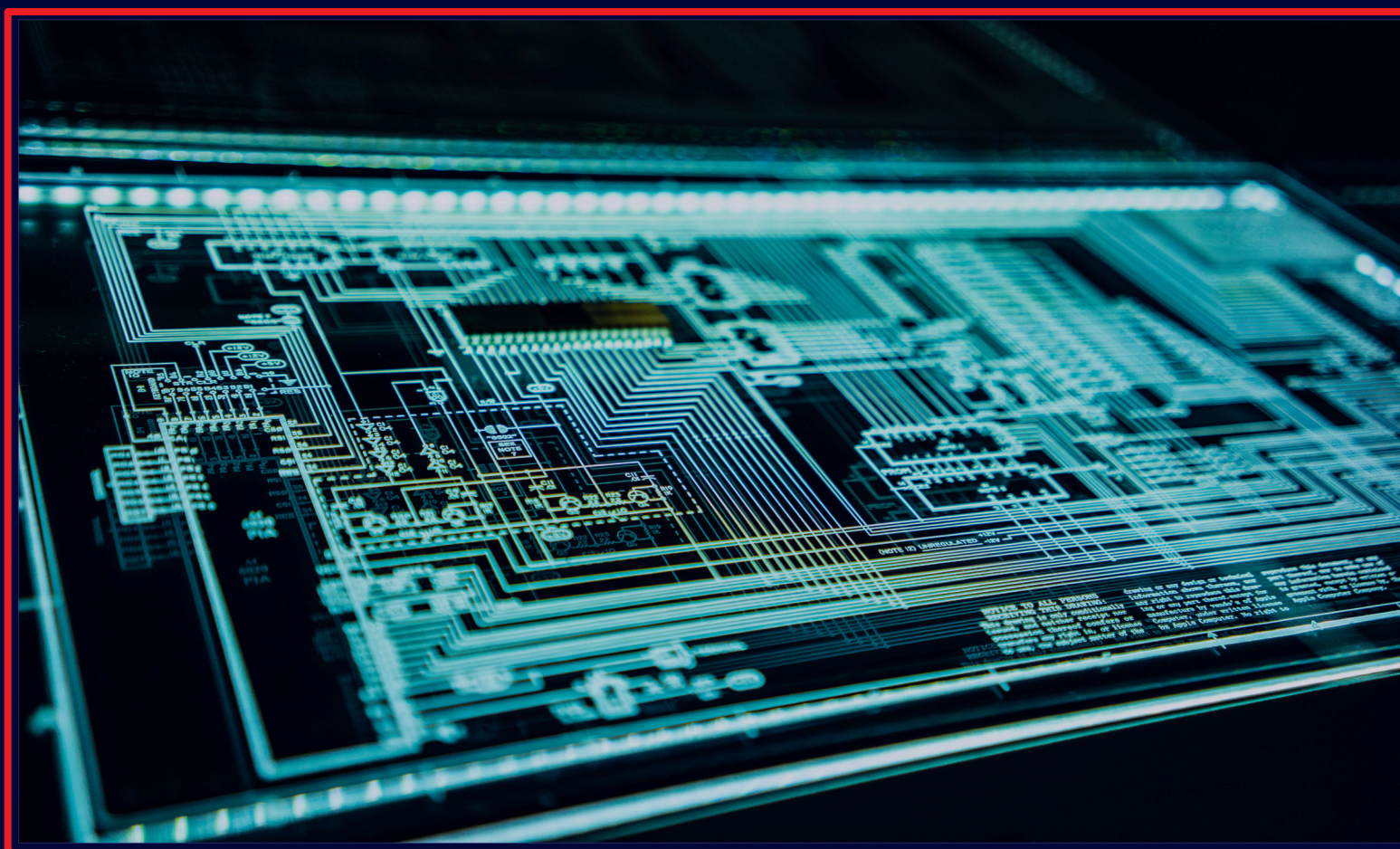
Obowiązująca ustawa o krajowym systemie cyberbezpieczeństwa implementująca do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych oraz Rozporządzenie Parlamentu Europejskiego i Rady (UE) w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (tzw. RODO) wymuszają na MŚP intensywne działania w zakresie cyberbezpieczeństwa. Bezpieczeństwo prowadzenia biznesu, jak również wymagania klientów są w pewnej mierze oparte na cyberbezpieczeństwie, gdzie dojrzałość organizacji w tym zakresie staje się warunkiem rozpoczęcia kooperacji gospodarczej.



Odpowiedzią na problemy, wyzwania i potrzeby MŚP jest usługa w zakresie cyberbezpieczeństwa oferowana przez Stowarzyszenie Rozwoju Społeczno-Gospodarczego „Wiedza”, koordynatora Mazowieckiego Klastra ICT – Krajowego Klastra Kluczowego.



KRAJOWY
KLASTER
KLUCZOWY



Usługa:

Usługa została stworzona w ramach projektu pn. „innLOGY – wsparcie przedsiębiorstw o dużym potencjale technologicznym” realizowany w ramach projektu współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego, Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020 nr RPMA.03.01.02-14-b657/18, pn. "Modelowanie Systemu Ofert Dla Innowacji", Oś Priorytetowa III Rozwój potencjału innowacyjnego i przedsiębiorczości, Działanie 3.1 Poprawa rozwoju MŚP na Mazowszu Poddziałanie 3.1.2 Rozwój MŚP.

Usługa została przetestowana przez cztery przedsiębiorstwa MŚP. Testerzy jednogłośnie wystawili wysoką ocenę jakości testowanej usługi, jak również docenili kompetencje i doświadczenie naszych ekspertów. Cztery powyższe studia przypadku pozwoliły na zbudowanie komercyjnej specyfikacji usługi w zakresie cyberbezpieczeństwa.

Cel usługi:

Ocena stanu cyberbezpieczeństwa środowiska teleinformatycznego Klienta oraz identyfikacja i analiza luk zgodności z wymaganiami i standardami.

Obszary usługi:

- Infrastruktura
- Zarządzanie bezpieczeństwem informacji
- Incydenty bezpieczeństwa
- Zarządzanie ciągłością działania
- Utrzymanie systemów

**Korzyści klienta, czyli rezultat
wyświadczonej usługi
doradczej:**

Klient otrzyma przedmiotową opinię o swoim przedsiębiorstwie w zakresie cyberbezpieczeństwa, ocenę poszczególnych kluczowych obszarów, wykaz zidentyfikowanych elementów niepożądanych wraz ze stosownymi rekomendacjami. Usługa pozwoli z jednej strony na analizę aktualnego stanu zabezpieczeń i procedur stosowanych przez klienta, zaś z drugiej strony dostarczy informacji potrzebnych do przygotowania planu wdrożenia niezbędnych działań naprawczych.

Sposób realizacji usługi:

Usługa jest realizowana przez wykwalifikowanych konsultantów, którzy ściśle współpracują z klientem. Indywidualnie ustalony harmonogram prac w ramach usługi składa się z: określenia planu prac, realizacji części doradczej stacjonarnie u klienta, analizy potencjalnych niezgodności, przygotowania raportu z usługi, podsumowania usługi i omówienia raportu z klientem.



Kontakt:

Projekt innLOGY umożliwił publikację cyklu artykułów poświęconych bezpieczeństwu cybernetycznemu. Zachęcamy do odwiedzenia naszych mediów społecznościowych oraz strony internetowej, gdzie znajdziecie sporą dawkę wiedzy oraz szereg porad zabezpieczających Wasze przedsiębiorstwo przed wirtualnymi zagrożeniami.

Dane kontaktowe:

Mazowiecki Klaster ICT

ul. Piękna 31/37

00-677, Warszawa

Tel. +48 512 998 804

e-mail: biuro@klasterict.pl

Strona WWW: www.klasterict.pl

Stowarzyszenie Rozwoju Społeczno-Gospodarczego "Wiedza"

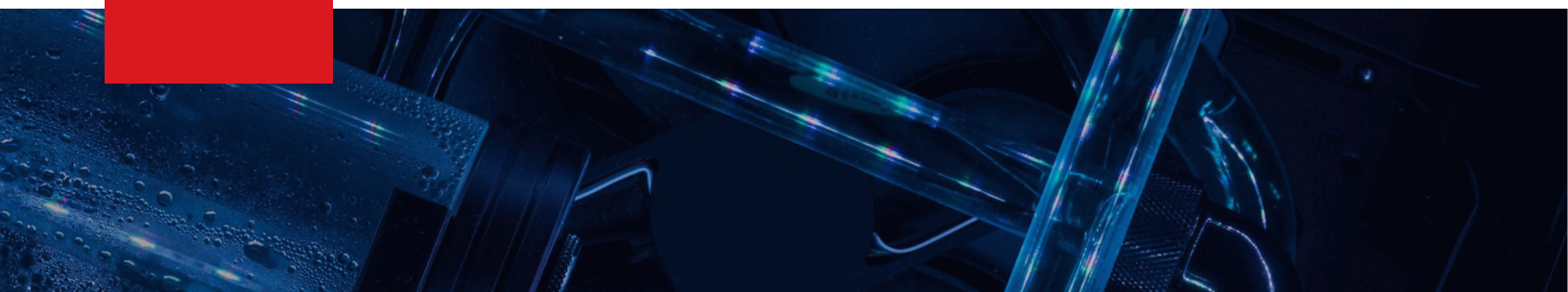
ul. Piękna 31/37

00-677, Warszawa

Tel. +48 512 196 378

e-mail: biuro@klasterict.pl

Strona WWW: www.stowarzyszenie-wiedza.pl



Projekt pn. „innLOGY – wsparcie przedsiębiorstw o dużym potencjale technologicznym” realizowany w ramach projektu współfinansowanego ze środków Europejskiego Funduszu Rozwoju Regionalnego, Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020 nr RPMA.03.01.02-14-b657/18, pn. "Modelowanie Systemu Ofert Dla Innowacji", Oś Priorytetowa III Rozwój potencjału innowacyjnego i przedsiębiorczości, Działanie 3.1 Poprawa rozwoju MŚP na Mazowszu Poddziałanie 3.1.2 Rozwój MŚP.



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego

