T Business

Cyberbezpieczeństwo w praktyce

– przewodnik dla gmin i wodociągów

Connecting your world.

Cybersecurity

Jak możemy Ci pomóc?

Dobierzemy odpowiednie rozwiązania w zakresie cyberbezpieczeństwa **dopasowane do potrzeb Twojej jednostki.**

Oferujemy kompleksowe wsparcie techniczne i formalne – od przygotowania wniosku aż po realizację inwestycji.

Zapewnimy zgodność z obowiązującymi normami i wymaganiami regulacyjnymi.

Nie musisz posiadać własnego zespołu ds. cyberbezpieczeństwa – **nasi eksperci przeprowadzą Cię przez cały proces**, od planowania po wdrożenie i utrzymanie.

Bezpieczeństwo Twojego systemu zaopatrzenia w wodę zaczyna się od dobrego planu.

- **Nowy program dofinansowania**
- **Okres realizacji wydatków: od 1 stycznia 2025 r. do 30 czerwca 2026 r.**
- **Budżet programu: 328,5 mln zł netto**

Co to oznacza w praktyce?

Trwający nabór w ramach Inwestycji C3.1.1. KPO to szansa na pozyskanie środków na wdrożenie nowoczesnych zabezpieczeń i spełnienie wymogów regulacyjnych.

Pomagamy w doborze rozwiązań dopasowanych do potrzeb jednostki pod kątem zapewnienia cyberbezpieczeństwa oraz spełnienia norm regulacyjnywch.

Skontaktuj się z nami!

Formularz kontaktowy

Na co można otrzymać dofinansowanie?

Szkolenia z cyberbezpieczeństwa

Tworzenie planów i procedur bezpieczeństwa

Oprogramowanie do monitorowania zagrożeń

Bezpieczne połączenia zdalne

Kopie zapasowe danych

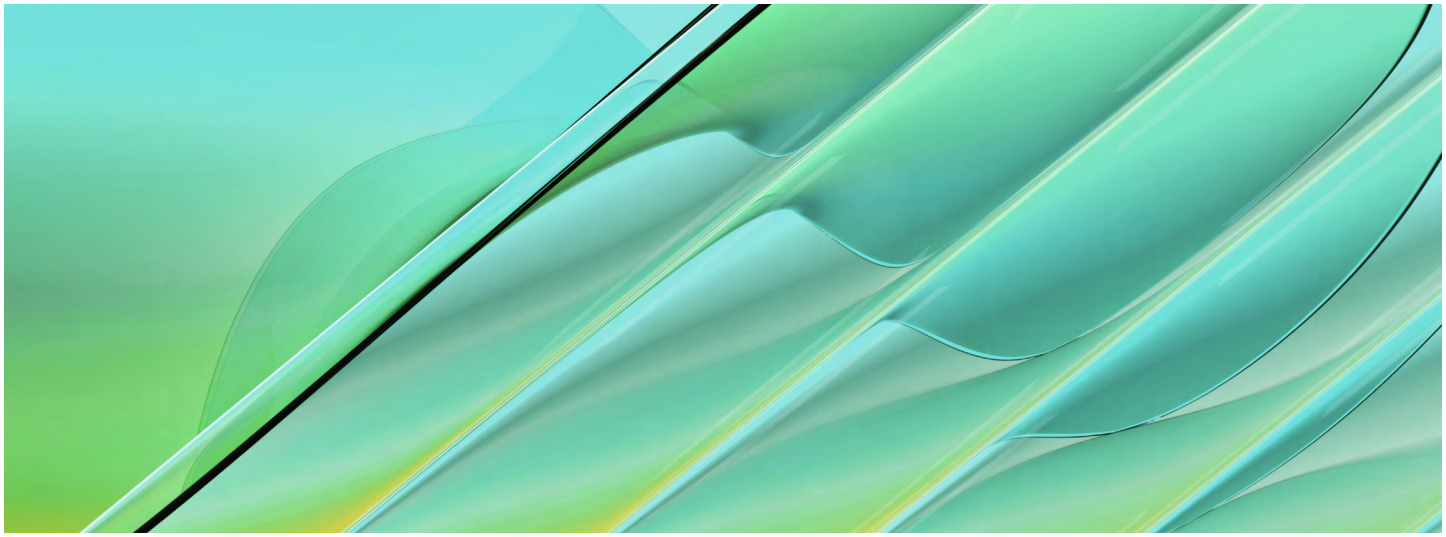
Oddzielenie sieci wodociągowej od sieci biurowej

Audyty i testy bezpieczeństwa

Powody uruchomienia programu

- Wzrastająca liczba ataków wymierzonych m.in. w wodociągi i kanalizację.
- Możliwość wystąpienia poważnych zakłóceń w działaniu systemów – w niektórych przypadkach cyberprzestępcy manipulowali parametrami urządzeń, ustawiając je na maksymalne wartości.
- Dyrektywa NIS 2 – wprowadzenie nowych obowiązków dla podmiotów kluczowych i ważnych oraz rozbudowanych środków nadzoru i egzekwowania przepisów.

- **Wsparcie podmiotów, które:**
  - prowadzą działalność w zakresie zbiorowego zaopatrzenia w wodę,
  - są objęte Krajowym Systemem Cyberbezpieczeństwa (KSC),
  - wykorzystują technologie IT oraz OT,
  - korzystają z przemysłowych systemów sterowania (ICS),
  - potrzebują modernizacji i rozbudowy infrastruktury cyberbezpieczeństwa.



Obszary cyberbezpieczeństwa objęte dofinansowaniem, dostępne w ramach oferty T Business.

Organizacyjny

audyty, polityki i procedury bezpieczeństwa, systemy zarządzania ryzykiem, ciągłością działania i zgodnością IT/OT

1.1 Systemowe zarządzanie bezpieczeństwem i ciągłością działania IT/OT	Audyty
	Badania zgodności, np. z Dyrektywą NIS 2
	Program Zarządzania Podatnościami
	Profesjonalne doradztwo

Kompetencyjny

szkolenia i rozwój wiedzy z zakresu cyberbezpieczeństwa dla pracowników, kadry IT/OT oraz zarządzających

2.1 Szkolenia z zakresu cyberbezpieczeństwa (kolorem oznaczone rozwiązania premiowane)	**Security Awareness:** • Cyber Know • KnowBe4 • Uczymy rozpoznawać i reagować na próby manipulacji. • Wzmacniamy odporność na ataki wymierzone w pocztę służbową i telefony. • Kształtujemy bezpieczne nawyki w codziennej pracy. • Zmniejszamy ryzyko ataków socjotechnicznych. • Dopasowujemy treści do aktualnych zagrożeń i realiów organizacji.

Techniczny IT

zabezpieczenie infrastruktury IT: serwery, stacje robocze, dane, sieci, systemy bezpieczeństwa i backupy

3.1 Bezpieczeństwo systemów informatycznych	**Usługi Profesjonalne Bezpieczeństwa IT:** • Skanowanie podatności • Testy penetracyjne
3.2 Bezpieczeństwo WWW (stron i/lub platform internetowych)	
3.3 Bezpieczeństwo stacji roboczych	• Analiza Śledcza (Forensics) • AntyDDoS • Cyber Guard® • DLP • EDR • E-mail Secure Gateway • ITDR • MDR • NGFW (Next-Generation Firewall) • NDR • Oprogramowanie antywirusowe
3.4 Rozwiązanie bezpieczeństwa sieci	
3.5 Rozwiązania bezpieczeństwa styku sieci Internet z usługami wewnętrznymi	
3.6 Zwiększenie niezawodności i wydajności	

3.6 Rozwiązania sieciowe WAN/LAN/ Wi-Fi	• **Oprogramowanie do zarządzania tożsamością i dostępem:**
	  • IAM
	  • PIM
	  • NAC
	  • MFA, Klucze U2F

3.7 Rozwiązania wirtualizacyjne	
3.8 Rozwiązania kopii zapasowych	
3.9 Redundancja (HA)	• Program Zarządzania Podatnościami • Security Operations Center (SOC) • SIEM • SOC Lite • SOAR • Threat Intelligence • UTM • Web Application Firewall (WAF) • WEG • XDR • Zarządzany Firewall
3.10 Rozwiązania zarządzania operacyjnego	
3.11 Bezpieczeństwo komunikacji	
3.12 Monitorowanie bezpieczeństwa	
3.13 Reagowanie w zakresie bezpieczeństwa	
3.14 Zarządzanie uprawnieniami użytkowników	oraz inne rozwiązania dopasowane do indywidualnych potrzeb jednostki
3.15 Zabezpieczanie dowodów cyfrowych	

Techniczny OT

ochrona środowiska przemysłowego OT/ICS: systemy sterowania, IoT, sieci OT, monitoring, urządzenia w stacjach uzdatniania i punktach poboru wody

Profesjonalne doradztwo, rozwiązania dopasowane do indywidualnych potrzeb jednostki

Pomożemy Ci w doborze rozwiązań potrzebnych dla Twojej jednostki pod kątem **zapewnienia cyberbezpieczeństwa** oraz **spełnienia norm regulacyjnych, np. NIS 2. Zapewniamy wsparcie w wypełnianiu wniosków.**

Jak skorzystać z programu:

Krok 1	Krok 2	Krok 3	Krok 4	Krok 5
Sprawdź wymagania	Zaplanuj działania **KONTAKT**	Złóż wniosek	Zrealizuj projekt	Rozlicz i raportuj

Finansowanie

ALOKACJA – ponad 300 mln zł (netto), dofinansowanie 100% (brak wkładu własnego), VAT to wydatek niekwalifikowalny, dofinansowanie tylko na wydatki w kwocie netto.

ŹRÓDŁO FINANSOWANIA – Inwestycja C3.1.1. Krajowego Planu Odbudowy i Zwiększania Odporności (KPO).

Ramowy harmonogram konkursu grantowego

Etapy konkursu grantowego **CYBERBEZPIECZNE WODOCIĄGI**	2025 r. VIII	IX	X	XI	XII	2026 r. I	II	III	IV	V	VI
Ogłoszenie naboru wniosków do konkursu grantowego	■										
Nabór wniosków o grant	■	■									
Ocena wniosków		■	■	■							
Ogłoszenie listy rankingowej wniosków objętych wsparciem				■							
Zawieranie umów z grantobiorcami				■	■						
Przekazanie środków grantobiorcom (jedna transza)					■	■					
Realizacja projektów grantowych (**kwalifikowalność wydatków od 1.01.2025 r. do 30.06.2026 r.**)	■	■	■	■	■	■	■	■	■	■	■
Złożenie wniosku rozliczającego (**do 30.06.2026 r.**)											■

Ministerstwo Cyfryzacji

Terminy mogą ulec zmianie. Prosimy o ich weryfikację na stronie programu lub bezpośredni kontakt z przedstawicielem T-Mobile.

Słownik pojęć

Analiza śledcza (Forensics) – proces dochodzenia i analizy incydentów związanych z bezpieczeństwem IT. Polega na zbieraniu dowodów, identyfikowaniu źródła ataku, metod użytych przez cyberprzestępców, zabezpieczeniu dowodów oraz określeniu zakresu i skutków ataku. Dodatkowo, pomaga w przygotowywaniu raportów niezbędnych do działań prawnych.

AntyDDoS – system chroniący przed atakami DDoS, które mają na celu przeciążenie strony internetowej lub systemu, aby uniemożliwić ich działanie lub atak na konkretną aplikację używaną przez firmę.

Cyber Guard® – autorskie i unikatowe rozwiązanie, wykorzystujące mechanizmy Big Data oraz uczenia maszynowego w procesie monitorowania stanu bezpieczeństwa IT urządzeń mobilnych. Dzięki wykorzystaniu danych z sieci operatora umożliwia bezagentową ochronę urządzeń mobilnych przed złośliwym oprogramowaniem (malware), phishingiem oraz wyciekiem danych.

DLP (Data Loss Prevention) – technologia zapobiegająca wyciekowi wrażliwych danych z organizacji, np. blokuje wysyłanie PESEL-i czy numerów kont poza firmę przez nieupoważnionego pracownika lub niewskazaną do tego aplikację.

EDR (Endpoint Detection and Response) – zaawansowane oprogramowanie do monitorowania komputerów i serwerów (tzw. urządzeń końcowych), które wykrywa i reaguje na nietypowe zachowania, mogące świadczyć o zagrożeniu.

E-mail Secure Gateway – rozwiązanie bezpieczeństwa poczty e-mail, chroniące przed spamem, phishingiem i załącznikami złośliwego oprogramowania.

ITDR (Identity Threat Detection and Response) – rozwiązanie do wykrywania i reagowania na zagrożenia związane z tożsamościami cyfrowymi użytkowników, np. przejęcie konta, nadużycie uprawnień.

MDR (Managed Detection and Response) – usługa, w ramach której zewnętrzny zespół specjalistów monitoruje środowisko organizacji, wykrywa zagrożenia i reaguje na nie w czasie rzeczywistym.

NGFW (Next-Generation Firewall) – zapora nowej generacji, która poza filtrowaniem ruchu sieciowego analizuje też aplikacje, użytkowników i szyfrowany ruch. Może wykrywać ataki i złośliwe działania.

NDR (Network Detection and Response) – system analizujący ruch sieciowy w czasie rzeczywistym, aby wykryć nietypowe zachowania i potencjalne ataki na poziomie sieci.

Oprogramowanie antywirusowe – program chroniący komputer lub serwer przed znanym złośliwym oprogramowaniem (np. wirusami, trojanami).

Oprogramowanie do zarządzania tożsamością i dostępem – zestaw rozwiązań służących do kontrolowania, kto i w jaki sposób może korzystać z systemów informatycznych:

- **IAM (Identity & Access Management)** – zarządzanie użytkownikami i ich dostępami do systemów;
- **PIM (Privileged Identity Management)** – kontrola dostępu do kont uprzywilejowanych (z wysokimi uprawnieniami);
- **NAC (Network Access Control)** – system sprawdzający, czy urządzenie może uzyskać dostęp do sieci;
- **MFA (Multi-Factor Authentication), Klucze U2F** – logowanie wieloskładnikowe (np. hasło + telefon) lub z użyciem fizycznych kluczy bezpieczeństwa.

Program Zarządzania Podatnościami – celem usługi jest minimalizacja ryzyka wystąpienia zagrożenia poprzez identyfikację oraz mitygację podatności w środowisku IT klienta; podatności to „słabe punkty” w infrastrukturze IT, które mogą być wykorzystane do przeprowadzenia ataku przez cyberprzestępców.

Security Awareness (Budowanie świadomości cyberzagrożeń) – działania edukacyjne zwiększające wiedzę pracowników o zagrożeniach i bezpiecznych zachowaniach:

- **Cyber Know** – autorskie rozwiązanie T-Mobile służące do wzmacniania kultury cyberbezpieczeństwa w organizacji; umożliwia przeprowadzanie realistycznych symulacji ataków phishingowych (e-mail) i smishingowych (SMS), które pozwalają zidentyfikować podatności wśród pracowników i podnieść ich odporność na cyberzagrożenia;
- **KnowBe4** – kompleksowa platforma zawierająca bogatą bibliotekę szkoleń i materiałów do transferu wiedzy. Pomaga w kształtowaniu kultury bezpieczeństwa w organizacjach i realizacji programów do minimalizacji zagrożeń czynnika ludzkiego.

Security Operations Center (SOC) – centrum monitorowania bezpieczeństwa w trybie 24/7/365. Usługa pozwala na identyfikację potencjalnego zagrożenia, wskazanie miejsca jego wystąpienia i poziomu krytyczności oraz poinformowanie o tym fakcie w postaci wygenerowanego alarmu. Dzięki temu możliwe jest podjęcie szybkiej reakcji i minimalizacja negatywnych skutków zdarzenia. W ramach usługi jednostki zyskują dostęp do specjalistów z zakresu bezpieczeństwa.

SIEM (Security Information and Event Management) – system zbierający i analizujący logi (zdarzenia) z różnych urządzeń, pomagający szybko wykryć niepokojące działania.

SOC Lite – uproszczona forma usługi SOC dostosowana do mniejszych organizacji – może bazować na gotowych scenariuszach i zewnętrznym monitoringu.

SOAR (Security Orchestration, Automation and Response) – system automatyzujący reakcję na incydenty, np. automatycznie blokuje użytkownika lub izoluje urządzenie w przypadku wykrycia zagrożenia.

Threat Intelligence – dane o znanych zagrożeniach (adresy IP, domeny, techniki ataków), które pomagają szybciej wykrywać i blokować potencjalne niebezpieczeństwa.

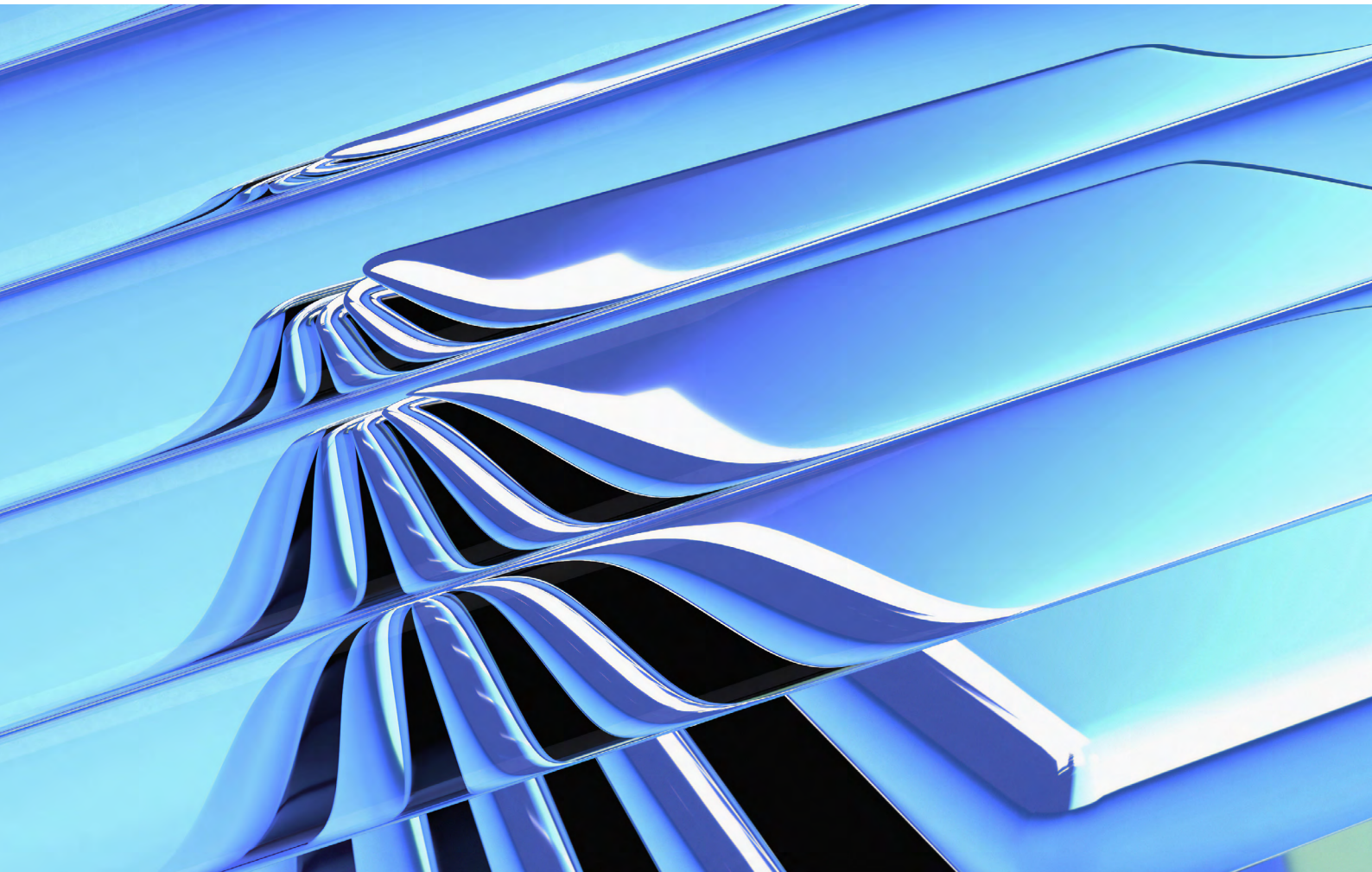
UTM (Unified Threat Management) – wielofunkcyjne urządzenie łączące kilka funkcji zabezpieczających: firewall, antywirus, filtrowanie treści, VPN itp.

Web Application Firewall (WAF) – zapora sieciowa chroniąca aplikacje internetowe, takie jak strony WWW, systemy logowania czy formularze, przed typowymi zagrożeniami, m.in. wstrzykiwaniem złośliwego kodu (np. SQL injection, XSS) oraz próbami nieautoryzowanego dostępu.

WEG (Web Filtering Gateway) – system kontroli dostępu do stron internetowych – może blokować np. strony pornograficzne, hazardowe, niebezpieczne lub rozpraszające uwagę.

XDR (Extended Detection and Response) – zintegrowana platforma łącząca informacje z wielu źródeł (komputery, sieć, konta użytkowników), aby skutecznie zapobiegać atakom i wykrywać anomalie w pracy użytkowników.

Zarządzany Firewall – usługa zewnętrznego zarządzania zaporą sieciową (np. NGFW) – dostawca ustawia reguły, monitoruje zdarzenia i reaguje w razie incydentów.



T Business

SKORZYSTAJ Z NASZEJ POMOCY

w przygotowaniu wniosku i wdrożeniu rozwiązań objętych dofinansowaniem

Zapraszamy do kontaktu z T-Mobile.
Prześlij do nas wypełniony formularz.

NAZWA JEDNOSTKI:

IMIĘ I NAZWISKO:

TELEFON:

E-MAIL:

NOTATKI:

Więcej informacji na temat dofinansowania:

T-Mobile Polska S.A.
ul. Marynarska 12
02-674 Warszawa

Więcej informacji o usługach:
www.biznes.t-mobile.pl

Numer jobu: 14255158