5 LAT - PUBLIKACJA JUBILEUSZOWA
DEPARTAMENT CYBERBEZPIECZEŃSTWA
MINISTERSTWO CYFRYZACJI

Ministerstwo Cyfryzacji

Spis treści

PWCyber - razem dla bezpiecznej przyszłości. Słowo wstępne Wicepremiera, Ministra cyfryzacji Krzysztofa Gawkowskiego

Szanowni Państwo,

z wdzięcznością oddaję w Państwa ręce niniejszą publikację, która podsumowuje pięć lat działania Programu Współpracy w Cyberbezpieczeństwie (PWCyber). Pięć lat dynamicznego rozwoju, który nie byłby możliwy bez ogromnego zaangażowania i szczególnej współpracy sektora publicznego i prywatnego. W dobie nieustannie zmieniającego się krajobrazu technologicznego i coraz bardziej zaawansowanych zagrożeń w cyberprzestrzeni, połączenie sił z sektorem prywatnym stało się kluczowe dla zapewniania bezpieczeństwa naszego kraju.

Program PWCyber narodził się z potrzeby stworzenia platformy, która połączy doświadczenie oraz ekspercką wiedzę firm technologicznych z sektorem publicznym. To przedsięwzięcie o charakterze niekomercyjnym o ogromnym znaczeniu strategicznym, ugruntowało swoją pozycję jako kluczowy i ważny element w rozwoju krajowego systemu cyberbezpieczeństwa. Obecnie, kiedy cyfrowa infrastruktura jest tak samo istotna jak fizyczne granice państwa, współpraca międzysektorowa to nie tylko dobra praktyka, ale wręcz konieczność.

W erze cyfryzacji, gdzie rozwój technologiczny następuje z zawrotną prędkością, sektor publiczny i prywatny muszą działać ramię w ramię, aby sprostać wspólnym wyzwaniom. Firmy technologiczne posiadają nie tylko zaawansowaną wiedzę techniczną, ale także doświadczenie w szybkim reagowaniu na nowe zagrożenia. Z kolei administracja publiczna, mająca na uwadze interesy społeczeństwa, zapewnia odpowiednie regulacje i polityki, które tworzą ramy dla bezpiecznego rozwoju cyfrowego. Razem tworzymy zintegrowany system, który jest odporny na ataki i zdolny do adaptacji w obliczu nowych wyzwań.

Przez pięć lat PWCyber zgromadził kilkadziesiąt firm operujących na rynku cyfrowym. Cieszymy się, że z roku na rok ta liczba rośnie, chociaż nie liczba partnerów jest najważniejsza a ilość wspólnych inicjatyw i działań na rzecz podnoszenia poziomu cyberbezpieczeństwa kraju. Nasza inicjatywa jest otwarta i gotowa na rozwijanie współpracy z obecnymi i wszystkimi nowymi partnerami, którzy dołączą do Programu. Dotychczasowe wspólne działania przyniosły imponujące rezultaty. Od 2020 roku dzięki zaangażowaniu partnerów przeprowadziliśmy 77 szkoleń, w których uczestniczyło ponad 34 tysiące osób, w tym specjaliści IT z administracji państwowej, samorządów, szpitali i placówek ochrony zdrowia. Przekazana wiedza przyczynia się do podnoszenia kompetencji z zakresu cyberbezpieczeństwa i budowania silnego systemu cyberbezpieczeństwa w Polsce, zdolnego do skutecznego przeciwdziałania zagrożeniom.

Statystyki pokazują, że wyzwań nie brakuje. W 2022 roku zarejestrowano 40 tysięcy incydentów cyberbezpieczeństwa, a w 2023 roku liczba ta podwoiła się. W pierwszym półroczu 2024 roku obserwujemy dalszy wzrost, co jednoznacznie potwierdza, że jesteśmy na wojnie w cyberprzestrzeni. W takiej rzeczywistości poczucie odpowiedzialności i gotowość do działania są kluczowe. Współpraca w ramach PWCyber to dowód, że razem możemy stawić czoła zagrożeniom i skutecznie chronić naszą cyfrową suwerenność.

Dziękuję wszystkim partnerom, ekspertom i instytucjom za ich wkład w budowanie bezpiecznej, cyfrowej Polski. Wasza determinacja i zaangażowanie są niezastąpione. Zapraszam do lektury tej publikacji, która nie tylko podsumowuje nasze dotychczasowe osiągnięcia, ale również ukazuje drogę, jaką chcemy podążać w przyszłości.

Wicepremier, Minister cyfryzacji
Krzysztof Gawkowski

Od wizji do rzeczywistości - 5 lat Programu Współpracy w Cyberbezpieczeństwie. Słowo wstępne Wiceministra Pawła Olszewskiego

Szanowni Państwo,

kiedy w 2019 roku ruszał Program Współpracy w Cyberbezpieczeństwie (PWCyber), kierowała nim wizja: stworzyć silne i innowacyjne partnerstwo, które pomoże wpierać bezpieczeństwo Polski w coraz bardziej złożonym cyfrowym świecie. W 2024 roku, po pięciu latach dynamicznej współpracy, możemy z dumą stwierdzić, że ta wizja staje się rzeczywistością.

W świecie, gdzie technologia przenika wszystkie aspekty naszego życia, cyberbezpieczeństwo jest nie tylko wyzwaniem technicznym, ale także społecznym. To odpowiedzialność, którą dzielimy wszyscy: sektor publiczny i prywatny, organizacje i obywatele. Każdy z nas odgrywa istotną rolę w zapewnieniu bezpiecznej cyfrowej przestrzeni.

Program PWCyber został stworzony jako odpowiedź na te wyzwania, łącząc siły sektora publicznego i prywatnego. To partnerstwo, które pozwala nam korzystanie z najlepszych praktyk i najnowszych osiągnięć technologicznych. Dzięki współpracy z liderami branży IT i ekspertami w dziedzinie bezpieczeństwa, udało się zwiększyć świadomość w podejściu do ochrony cyfrowej.

W obliczu coraz bardziej złożonych wyzwań, jakie niesie ze sobą współczesny świat, podnoszenie kompetencji stało się naszym priorytetem. Wspólnie organizujemy szkolenia i warsztaty, które mają nie tylko zwiększyć świadomość zagrożeń, ale także wyposażyć nas w umiejętności niezbędne do skutecznego przeciwdziałania atakom w cyberprzestrzeni.

Identyfikacja podatności jest kluczem do zachowania bezpieczeństwa w dynamicznie zmieniającym się środowisku technologicznym. Poprzez regularną wymianę informacji, stajemy się bardziej odporni na potencjalne incydenty, wzmacniając tym samym naszą gotowość na wszelkie wyzwania.

Promowanie innowacyjnych rozwiązań jest fundamentem naszej strategii rozwoju. Wspieramy projekty, które przyczyniają się do poprawy stanu cyberbezpieczeństwa.

Niech te działania będą dowodem naszego zaangażowania w budowanie bezpiecznego i innowacyjnego cyfrowego kraju. Razem jesteśmy w stanie sprostać wszelkim wyzwaniom i zagrożeniom, które stają przed nami.

Przyszłość stawia przed nami wiele wyzwań, ale także oferuje niezwykłe możliwości. W erze globalnych sieci i cyfrowej transformacji, nasze działania muszą być sprawne i dalekowzroczne. Zwiększona liczba incydentów, które odnotowaliśmy w ostatnich latach, przypomina nam o wadze naszej misji i konieczności nieustannego doskonalenia.

Pragnę wyrazić moje najgłębsze podziękowania dla wszystkich partnerów, ekspertów i instytucji, które przyczyniają się do rozwoju PWCyber.

Paweł Olszewski
Wiceminister cyfryzacji

Znaczenie współpracy w cyberbezpieczeństwie - Dyrektor Departamentu Cyberbezpieczeństwa, Łukasz Wojewoda

Szanowni Państwo,

w zakresie cyberbezpieczeństwa nie ma nic ważniejszego niż współpraca i należy to bardzo wyraźnie podkreślić. Do świata o wysokim ryzyku związanym z cyberbezpieczeństwem powinniśmy się już przyzwyczaić. Cyberataków jest coraz więcej, ale nie jesteśmy bezbronni i udaje nam się skutecznie przeciwdziałać cyberzagrożeniom. Razem możemy skuteczniej stawiać czoło wyzwaniom. Program Współpracy w Cyberbezpieczeństwem (PWCyber) jest najlepszym przykładem skutecznych działań na rzecz bezpiecznej cyberprzestrzeni kraju, których filarem jest kooperacja sektora publicznego z sektorem prywatnym.

Program PWCyber stał się jednym z kluczowych elementów budowania bezpiecznej, cyfrowej przyszłości naszego kraju. Przez ostatnie 5 lat wspólnie z naszymi partnerami PWCyber - instytucjami z sektora publicznego i prywatnego oraz ekspertami z dziedziny bezpieczeństwa teleinformatycznego, stworzyliśmy wyjątkową platformę współpracy. Platformę, która aktywnie wspiera rozwój wiedzy, dobrych praktyk, budowania kompetencji w zakresie cyberbezpieczeństwa, a także stawia na ważny aspekt dzielenia się informacją, aby w porę zapobiegać i sprawnie reagować na skutki incydentów. Nasze wspólne działania pozwoliły na zwiększenie świadomości w zakresie zagrożeń występujących w cyberprzestrzeni oraz na zbudowanie solidnych fundamentów dla dalszego rozwoju i innowacji w tym obszarze.

Przykładów wspólnych działań w ramach PWCyber jest bardzo wiele i nie sposób ich wszystkich przytoczyć, jednakże niniejsza publikacja jest świadectwem tych osiągnięć i dowodem na to, jak wiele można zdziałać dzięki skutecznej współpracy, zaangażowaniu i otwartości naszych partnerów. Mam nadzieję, że znajdą w niej Państwo inspirację oraz motywację do dalszego działania na rzecz wzmacniania cyberbezpieczeństwa RP, które jest stałym wyzwaniem dla nas wszystkich. W dalszej perspektywie PWCyber będzie koncentrował się na zagadnieniach związanych z wykorzystaniem nowych technologii w dbaniu o cyberbezpieczeństwo i inicjował nowe rozwiązania na dynamicznie zmieniający się krajobraz tej sfery.

Dziękuję wszystkim partnerom, którzy przyczynili się do sukcesu PWCyber. Wasze zaangażowanie stanowi siłę napędową tego Programu.

Łukasz Wojewoda
Dyrektor Departamentu Cyberbezpieczeństwa
Ministerstwo Cyfryzacji

O Programie PWCyber

Program Współpracy w Cyberbezpieczeństwie (PWCyber) to realizowana przez Ministra Cyfryzacji inicjatywa o charakterze wymiany partnerskiej z sektorem prywatnym.

Celem Programu jest wzmocnienie krajowego systemu cyberbezpieczeństwa Rzeczpospolitej Polskiej poprzez współpracę międzysektorową. Obecnie Program zrzesza 48 firm technologicznych i organizacji, zarówno krajowych, jak i międzynarodowych, które wspólnie działają na rzecz zwiększenia bezpieczeństwa cyfrowych procesów oraz podnoszenia świadomości użytkowników o zagrożeniach w cyberprzestrzeni.

Podstawą współpracy w ramach PWCyber jest publiczna i transparentna formuła, która jest otwarta dla wszystkich podmiotów zainteresowanych rozwojem krajowego systemu cyberbezpieczeństwa. Wszyscy partnerzy funkcjonują na jednakowych zasadach, z zachowaniem tego samego formatu porozumień, które niezmiennie obowiązują od początku istnienia Programu.

Od ponad 5 lat, Program PWCyber stanowi platformę wymiany wiedzy eksperckiej, umożliwiając podnoszenie kompetencji w zakresie świadomości zagrożeń, metod ataków w cyberprzestrzeni oraz przeciwdziałania im. Program skupia się również na aspektach prawnych, organizacyjnych i technicznych, pomagając w rozwoju umiejętności potrzebnych do ochrony systemów i sieci teleinformatycznych.

Współpraca między Ministerstwem Cyfryzacji a sektorem prywatnym w ramach Programu PWCyber przynosi wymierne korzyści. Dzięki wspólnym działaniom i wymianie wiedzy, partnerzy Programu przyczyniają się do rozwoju kompetencji w zakresie cyberbezpieczeństwa oraz wdrażania nowoczesnych rozwiązań w sektorze publicznym, co jest kluczowe w obliczu dynamicznie zmieniających się wyzwań technologicznych.

Zgodnie z art. 45 ust. 1 pkt 2 ustawy o krajowym systemie cyberbezpieczeństwa, minister właściwy ds. informatyzacji odpowiada za rekomendowanie obszarów współpracy z sektorem prywatnym w celu zwiększenia cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Aby zapewnić realizację tego zadania, w 2019 r. ówczesny Minister Cyfryzacji oraz Pełnomocnik Rządu ds. Cyberbezpieczeństwa uruchomił Program Współpracy w Cyberbezpieczeństwie (PWCyber), jako jedno z działań w ramach powierzonych zadań.

Program wpisuje się także w cele Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, cel szczegółowy 3.2 „Nastawienie na rozwój współpracy między sektorem publicznym i prywatnym".

Program PWCyber ze względu na konieczność budowania zaufanych relacji z partnerami technologicznymi, jest otwarty dla firm z państw Unii Europejskiej, Organizacji Traktatu Północnoatlantyckiego i państw partnerskich NATO.

Obszary współpracy w ramach Programu PWCyber:

Obszar 1.
Podnoszenie kompetencji podmiotów krajowego systemu cyberbezpieczeństwa w zakresie świadomości zagrożeń, metod ataków w cyberprzestrzeni oraz prawnych, organizacyjnych i technicznych umiejętności przeciwdziałania zagrożeniom w systemach i sieciach teleinformatycznych.

Obszar 2.
Identyfikacja podatności i zagrożeń, wymiana informacji oraz wypracowywanie metod zgłaszania i obsługi incydentów, w tym również organizacja i udział w ćwiczeniach.

Obszar 3.
Opracowywanie rekomendacji w zakresie konfiguracji urządzeń, oprogramowania i usług w sposób maksymalizujący skuteczność mechanizmów zabezpieczających (ang. Security Baselines).

Obszar 4.
Przygotowanie i prowadzenie oceny oraz certyfikacji cyberbezpieczeństwa produktów i usług.

Obszar 5.
Promowanie innowacyjnych rozwiązań i projektów w dziedzinie cyberbezpieczeństwa oraz budowanie partnerstwa z podmiotami Krajowego Systemu Cyberbezpieczeństwa zainteresowanymi opracowywaniem, testowaniem i wdrażaniem nowych rozwiązań.

Inicjatywy prowadzone w ramach Programu PWCyber

W ramach Programu prowadzone są różnorodne inicjatywy, które mają na celu wsparcie i rozwój kompetencji kadr krajowego systemu cyberbezpieczeństwa. Szkolenia, będące jedną z najważniejszych aktywności, pozwalają uczestnikom zdobywać niezbędną wiedzę i umiejętności. Warsztaty oraz wizyty studyjne dodatkowo wzbogacają doświadczenie uczestników, umożliwiając im praktyczne zastosowanie zdobytej wiedzy oraz wymianę doświadczeń z ekspertami z branży.

Dzięki tym działaniom, Program PWCyber znacząco przyczynia się do wzrostu kompetencji i profesjonalizmu kadr w instytucjach dbających o cyberbezpieczeństwo, co w efekcie przekłada się na lepszą ochronę naszego państwa przed zagrożeniami w cyberprzestrzeni.

Warsztaty i wizyty studyjne

1. Partnerzy Programu przygotowują materiały merytoryczne które są publikowane w bazie wiedzy o cyberbezpieczeństwie na portalu gov.pl - cyber.gov.pl. Dotychczas w bazie wiedzy zamieściliśmy 18 poradników i rekomendacji, których autorami byli: **Cisco, Dell, Hewlett Packard Enterprise Polska, Microsoft, Securitum Szkolenia**.

2. W ramach współpracy partnerzy dzielą się informacji o niepublikowanych podatnościach oraz planowanych poprawkach bezpieczeństwa, czy też zaleceniach i dobrych praktykach w zakresie odpowiedniej konfiguracji oprogramowania. Działanie to, bazujące na zaufaniu, pomaga zapobiegać materializacji potencjalnych incydentów w cyberprzestrzeni.

3. Firma **Microsoft** przyczyniła się do rozwoju kompetencji pracowników krajowego systemu cyberbezpieczeństwa poprzez organizację szkoleń dotyczących usług chmurowych i najnowszych produktów firmy związanych z bezpieczeństwiem, w tym dot. szyfrowania w chmurze, koncepcji zero trust, czy hardeningiem.

4. W ramach współpracy z firmą **Amazon Web Services** (AWS), w siedzibie Ministerstwa Cyfryzacji zorganizowano szkolenie „Tabletop Exercise", w którym udział wzięły wybrane podmioty krajowego systemy cyberbezpieczeństwa. Dzięki praktycznej formie, szkolenie zwiększyło wiedzę dotyczącą praktycznego wymiaru reagowania na incydenty oraz właściwej ścieżki obiegu informacji. Kolejną inicjatywą było uczestnictwo w zagranicznych konferencjach, np.: AWS re:Inforce, czy AWS Regulatory Summit. Z kolei podczas wizyty studyjnej w USA w jednej z siedzib firmy AWS, przedstawiciele polskiej delegacji zapoznali się z usługami chmurowymi i szczegółowymi aspektami związanymi z ich funkcjonalnością. Dzięki takim inicjatywom pracownicy Ministerstwa Cyfryzacji zwiększyli swoje praktyczne kompetencje w zakresie rozwiązań chmurowych, które w maju 2024 r. zaowocowały zdobyciem przez „MC Team" pierwszego miejsca w zawodach AWS DDoS Game Day w Monachium.

5. W ramach współpracy z firmą **IBM Polska** oraz **Sevenet** przedstawiciele Ministerstwa Cyfryzacji oraz krajowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) oraz Centrów Operacji Bezpieczeństwa (Security Operation Center - SOC) uczestniczyli w warsztatach zorganizowanych w centrum bezpieczeństwa IBM X-Force Command Center we Wrocławiu. Agenda spotkania obejmowała prezentację narzędzi informatycznych w SOC, procesu budowania SOC, zintegrowanych narzędzi cyberbezpieczeństwa w zakresie poszczególnych funkcjonalności, w tym również Cyber Threat Intelligence w ujęciu taktycznym i strategicznym.

6. Kolejną inicjatywą były warsztaty zorganizowane przez firmę **IBM Polska** oraz **Sevenet**, podczas których omówiono zagadnienia związane z budową sektorowych zespołów CSIRT. Uczestnicy - przedstawiciele m.in. ministerstw, mieli okazję do wymiany wiedzy na temat umiejscowienia sektorowego zespołu CSIRT w krajowym systemie cyberbezpieczeństwa, jego budowy, zakresu usług jakie taki zespół powinien oferować oraz niezbędnych narzędzi wspierających funkcjonowanie CSIRT-u sektorowego.

7. Ministerstwo Cyfryzacji we współpracy z firmą **Elproma** zorganizowało warsztat w tematyce jammingu/spoofingu GPS „Desynchronizacja OT/IT infrastruktury krytycznej z użyciem jammingu/spoofingu GPS – jak monitorować i zapobiegać". Spotkanie pozwoliło uczestnikom reprezentującym instytucje krajowego systemu cyberbezpieczeństwa zgłębić aktualny i ważny z perspektywy cyberbezpieczeństwa temat.

8. Firma **Yubico** przeprowadziła wewnętrzne warsztaty dla pracowników Ministerstwa Cyfryzacji dot. najpowszechniejszych cyberzagrożeń i metod dwuetapowej weryfikacji z użyciem m.in. kluczy bezpieczeństwa.

9. W ramach współpracy z firmą **Fortinet** w siedzibie Ministerstwa Cyfryzacji odbyły się warsztaty z przedstawicielami wybranych podmiotów krajowego systemu cyberbezpieczeństwa. W trakcie warsztatów omówiono zasady działania Supportu Fortinet oraz PSIRT Fortinet w szczególności w kontekście badania urządzeń narażonych na cyberatak. Zaprezentowano procedury postępowania przy badaniu incydentu oraz przywrócenia urządzenia do bezpiecznego działania. Eksperci wskazali również skuteczne sposoby komunikacji pomiędzy klientem, Suportem Fortinet oraz instytucjami wspierającymi klienta w trakcie i po incydencie bezpieczeństwa.

Szkolenia

Kluczowym obszarem współpracy przez ostatnie 5 lat było podnoszenie kompetencji podmiotów krajowego systemu cyberbezpieczeństwa w zakresie świadomości zagrożeń, metod ataków w cyberprzestrzeni oraz prawnych, organizacyjnych i technicznych umiejętności przeciwdziałania zagrożeniom w systemach i sieciach teleinformatycznych. Jedną ze sztandarowych inicjatyw PWCyber są bezpłatne, specjalistyczne szkolenia online, organizowane cyklicznie przez Ministerstwo Cyfryzacji we współpracy z partnerami Programu, które adresowane są do kadr podmiotów krajowego systemu cyberbezpieczeństwa. Podzielone są na trzy kategorie: szkolenia dotyczące podstaw cyberhigieny (poziom 100), szkolenia dla kadry zarządzającej i pracowników działów IT (poziom 200) oraz szkolenia dla specjalistów IT (poziom 300). W ich ramach uczestnicy mogą zdobywać wiedzę z zakresu ochrony przed cyberzagrożeniami, zarówno siebie jak i organizacji, reagowania na incydenty oraz stosowania konkretnych rozwiązań technologicznych.

Wspólnie z partnerami Programu **od 2020 r. zorganizowaliśmy 77 szkolenia**, w których łącznie **udział wzięło 34 073 osoby**. (2020 – 4; 2021 – 12; 2022 – 14; 2023 – 20; 2024 – 25), (2020 – 763; 2021 – 3 170; 2 022 – 4 221; 2023 – 9 059; 2024 – 16 860).

Prowadziliśmy także cykle szkoleniowe adresowane do konkretnych grup podmiotów funkcjonujących w ramach krajowego systemu cyberbezpieczeństwa. Pierwszym z nich w latach 2020-2021 był cykl szkoleń **dla operatorów usług kluczowych (OUK)**. Cykl składał się z 6 szkoleń, w których **udział wzięły 1 874 osoby**.

W latach 2023-2024 zrealizowaliśmy wspólnie cykl szkoleń **dla podmiotów publicznych realizujących działalność leczniczą**. Cykl obejmował 10 spotkań online, w których uczestniczyło łącznie **4 295 osób**.

Wybrane opinie uczestników szkoleń online

Szkolenia online prowadzone w ramach PWCyber cieszą się coraz większym zainteresowaniem. Z roku na rok wzrasta liczba ich uczestników, których opinie o realizowanych przez nas inicjatywach stanowią dla nas i naszych partnerów siłę napędową do budowania kolejnych cyklów szkoleniowych. Ankiety ewaluacyjne, które otrzymujemy po każdym szkoleniu, wskazują na bardzo wysoki poziom merytoryczny szkoleń. Poniżej przedstawiamy wybrane opinie uczestników z ponad 30 tys. dotychczas otrzymanych ankiet.

- *Doskonale poprowadzone szkolenie.*
- *Więcej takich szkoleń z kompetentnymi prowadzącymi*
- *Świetny ekspert, wspaniale przygotowany, przedstawiał temat z pasją, bardzo interesujący temat. Czekam z niecierpliwością na następny cykl szkoleń*
- *Jedno z najlepszych dotychczasowych jak nie najlepsze. Szacunek dla prowadzącego.*
- *Wspaniałe szkolenie, zwięzłe i konkretne.*
- *Szkolenie prowadzone przez Panów świetnie przygotowane, poprowadzone. Pigułka wiedzy nt. zarządzania kryzysowego w firmie*
- *Szkolenie bardzo ciekawe, rzeczowe*
- *Bardzo dobre podejście z dwoma prelegentami, dwa podejścia do tego tematu z punktu widzenia prawnika i praktyka.*
- *Szkolenie interesujące a sposób podania informacji perfekcyjny. Świetnie, że po szkoleniu dostajemy materiały.*
- *Szkolenie przeprowadzone w sposób profesjonalny.*
- *Tak trzymać! Liczę na kontynuowanie Waszych szkoleń na tak wysokim poziomie, jednocześnie w tak przyswajalnej formie.*
- *Szkolenia na wysokim poziome, godne uwagi.*
- *Jestem pod wrażeniem wysokiego poziomu szkolenia.*

Statystyki szkoleń

Ogólna liczba przeprowadzonych szkoleń oraz liczba uczestników

	2020	2021	2022	2023	2024	SUMA
Liczba szkoleń	4	12	14	20	27	77
Liczba uczestników	763	3170	4221	9059	16860	34 073

Liczba szkoleń według Partnerów

Partner Programu	Liczba szkoleń
CISCO INTERNATIONAL LIMITED	21
Polski Klaster Cyberbezpieczeństwa CyberMadeInPoland sp. z o.o.	11
Dell sp. z o.o.	8
Samsung Electronics Polska sp. z o.o.	7
Hewlett Packard Enterprise Polska sp. z o.o.	5
Fundacja Bezpieczna Cyberprzestrzeń	3
DAGMA sp. z o.o.	3
Dynacon sp. z o.o.	3
Fudo Security sp. z o.o.	2
Galach Consulting sp. z o.o.	2
Microsoft sp. z o.o.	2
Media sp. z o.o.	1
HackingDept sp. z o.o.	1
IBM Polska sp. z o.o.	1
Engave S.A.	1
Sevenet S.A.	1
SNOK Sp.z.o.o	1
Proget sp. z o.o.	1
Secawa sp. z o.o.	1
Krypton Polska sp. z o.o.	1
Elproma Elektronika sp. z o.o.	1

Tematy przeprowadzonych szkoleń – szkolenia dla podmiotów ksc

EDYCJA 2020			
Lp.	**Data**	**Partner**	**Temat**
1	12.11.2020	Fundacja Bezpieczna Cyberprzestrzeń	Cyberhigiena w pracy i nie tylko (100)
2	02.12.2020	Dell sp. z o.o.	Mechanizmy bezpieczeństwa infrastruktury serwerowej (200)
3	10.12.2020	Cisco International Limited	Skuteczne wykrywanie cyberataków przy wykorzystaniu skonsolidowanej architektury bezpieczeństwa (200)
4	17.12.2020	Cisco International Limited	Typowy dzień analityka bezpieczeństwa (studium przypadku) (300)

EDYCJA 2021			
Lp.	**Data**	**Partner**	**Temat**
5	03.02.2021	Samsung Electronics Polska Sp. Z O.O.	Nie daj się zhakować! Jak chronić siebie i urządzenia mobilne przed atakami (100)
6	17.02.2021	Fundacja Bezpieczna Cyberprzestrzeń	Bezpieczeństwo sieci WiFi okiem atakującego (100)
7	03.03.2021	Fundacja Bezpieczna Cyberprzestrzeń	OpenSource Firewall - przegląd funkcji i konfiguracji (300)
8	04.03.2021	Media sp. z o.o.	Informatyka śledcza w samorządach (200)
9	10.03.2021	Dell sp. z o.o.	Zaawansowane zabezpieczenie danych w serwerowniach lokalnych i wyniesionych (300)
10	07.04.2021	Cisco International Limited	Jak napisać swoją sygnaturę IPS-ową? - wykorzystanie systemu IPS do wykrywania i blokowania zagrożeń (300)
11	22.04.2021	DELL SP. Z O.O.	Bezpieczne przechowywanie i przetwarzanie danych wrażliwych w infrastrukturze IT (200)
12	20.05.2021	IBM POLSKA SP. Z O.O.	Automatyzacja bezpieczeństwa w infrastrukturze teleinformatycznej przy wykorzystaniu rozwiązania Ansible (300)
13	21.10.2021	Microsoft sp. z o.o.	Jaj zadbać o cyberbezpieczeństwa w instytucjach naukowych - przykłady dobrych praktyk (100)
14	26.10.2021	Cisco International Limited, Dynacon sp. z o.o.	Cele i źródła ataków na infrastrukturę OUK-OT - szkolenie inauguracyjne cyklu szkoleń dla OUK (200)

EDYCJA 2022			
Lp.	**Data**	**Partner**	**Temat**
15	22.03.2022	Samsung Electronics Polska Sp. Z O.O.	Nie daj się zhakować! Jak chronić siebie i urządzenia mobilne przed atakami (100)
16	05.04.2022	Samsung Electronics Polska Sp. Z O.O.	Zarządzanie zdalne urządzeniami mobilnymi (200)
17	10.05.2022	Samsung Electronics Polska Sp. Z O.O.	Praktyczne rozwiązania ochrony urządzeń mobilnych (200)
18	24.05.2022	HackingDept sp. z o.o.	Jak rozpoznać i wykryć złośliwe urządzenia w organizacji? (200)
19	20.10.2022	Cisco International Limited	Data Center
20	03.11.2022	DELL SP. Z O.O.	Jak zapewnić odtworzenie danych? Bezpieczny backup w praktyce - szkolenie dwuczęściowe (1/2) (200)
21	08.11.2022	DELL SP. Z O.O.	Czego możemy oczekiwać od systemu backup-u? - szkolenie dwuczęściowe (2/2) (200)
22	17.11.2022	Fudo Security sp. z o.o.	Filozofia Zero Trust. Dlaczego VPN nie jest wystarczający w erze pracy zdalnej (200)
23	24.11.2022	Cisco International Limited	Bezpieczeństwo w sieciach przewodowych i bezprzewodowych 1/2 (200)
24	01.12.2022	Polski Klaster Cyberbezpieczeństwa CyberMadeInPoland sp. z o.o., Axence	Bezpieczeństwo stacji roboczych podstawą cyberbezpieczeństwa (200)
25	08.12.2022	Cisco International Limited	Bezpieczeństwo w sieciach przewodowych i bezprzewodowych 2/2 (200)
26	15.12.2022	Polski Klaster Cyberbezpieczeństwa CyberMadeInPoland sp. z o.o., Cypherdog	Szyfrowanie szyfrowaniem, ale kto ma klucze? (200)

EDYCJA 2023			
Lp.	**Data**	**Partner**	**Temat**
27	12.01.2023	Polski Klaster Cyberbezpieczeństwa CyberMadeInPoland sp. z o.o.	Dezinformacja – mechanizmy, skutki, przeciwdziałanie – Instytut Kościuszki
28	02.02.2023	Polski Klaster Cyberbezpieczeństwa CyberMadeInPoland sp. z o.o.	Cyberbezpieczeństwo w kontekście wymagań ustawy KSC - PBSG
29	02.03.2023	DELL SP. Z O.O.	Atak cyfrowy! Jak przetrwać? Co dalej? - Daniel Olkowski
30	06.04.2023	Hewlett Packard Enterprise Polska sp. z o.o.	Bezpieczeństwo Infrastruktury Informatycznej - zabezpieczenia serwerów
31	20.04.2023	Polski Klaster Cyberbezpieczeństwa CyberMadeInPoland sp. z o.o.	Jak skutecznie zaprojektować obsługiwać i rozwijać proces zarządzania incydentami bezpieczeństwa
32	27.04.2023	Cisco International Limited	Standaryzacja i automatyzacja kluczem do bezpiecznej sieci – część 1
33	18.05.2023	DELL SP. Z O.O.	Elementarz administratora/architekta pamięci masowych
34	25.05.2023	Cisco International Limited	Standaryzacja i automatyzacja kluczem do bezpiecznej sieci – część 2
35	01.06.2023	Axence, Polski Klaster Cyberbezpieczeństwa CyberMadeInPoland sp. z o.o.	Zdalna pomoc wobec pracy zdalnej – dobre praktyki helpdesku i zarządzania IT wobec nowych wymogów prawa
36	22.06.2023	Hewlett Packard Enterprise Polska sp. z o.o.	Mechanizmy zabezpieczenia dostępu do sieci LAN/WiFi
37	05.10.2023	DAGMA SP. Z O.O.	Chroń sieci przemysłowe (IT/OT) - jak chronić infrastrukturę krytyczną
38	12.10.2023	Galach Consulting sp. z o.o.	Obrona przed atakami socjotechnicznymi
39	19.10.2023	Hewlett Packard Enterprise Polska sp. z o.o.	Jak budować bezpieczne centrum przetwarzania danych
40	26.10.2023	Samsung Electronics Polska Sp. Z O.O.	Cyberhigiena urządzeń mobilnych
41	23.11.2023	Fudo Security sp. z o.o.	Zarządzanie Bezpieczeństwem Dostępu. Wprowadzenie do PAM i Zagrożeń Third Party
42	30.11.2023	Axence, Polski Klaster Cyberbezpieczeństwa CyberMadeInPoland sp. z o.o.	Jak edukować i uświadamiać użytkowników – wiedza jako podstawa cyberbezpieczeństwa
43	14.12.2023	Hewlett Packard Enterprise Polska sp. z o.o.	Zabezpieczenie danych przed ransomware z wykorzystaniem rozwiązań sprzętowych

EDYCJA 2024			
Lp.	**Data**	**Partner**	**Temat**
44	11.01.2024	Samsung Electronics Polska Sp. Z O.O.	Cyberbezpieczeństwo i zarządzanie urządzeniami mobilnymi
45	08.02.2024	DAGMA SP. Z O.O.	Ochrona przed współczesnymi atakami sieciowymi
46	15.02.2024	Samsung Electronics Polska Sp. Z O.O.	Zarządzanie urządzeniami mobilnymi - część 2
47	22.02.2024	Engave S.A.	Podnoszenie świadomości w zakresie cyberbezpieczeństwa. Metody rozpoznawania i zapobiegania atakom phishingowym, ransomware, malware
48	29.02.2024	SEVENET S.A.	Jak zabezpieczyć serwer pocztowy przed phishingiem
49	07.03.2024	Galach Consulting sp. z o.o.	Identyfikowanie i usuwanie podatności w systemach informatycznych
50	28.03.2024	DISKUS, Polski Klaster Cyberbezpieczeństwa CyberMadeInPoland sp. z o.o.	Jak skutecznie i bezpiecznie usunąć dane z elektronicznych nośników pamięci?
51	04.04.2024	DELL SP. Z O.O.	Narzędzia i technologie zwiększające cyberbezpieczeństwo urządzeń klienckich
52	11.04.2024	Proget sp. z o.o.	Budowanie świadomości w zakresie bezpieczeństwa i zarządzania mobilnością w organizacji
53	18.04.2024	Secawa sp. z o.o.	Nie tylko phishing, czyli co jeszcze grozi nam ze strony hakerów
54	23.04.2024	Microsoft sp. z o.o.	Zero Trust: zarządzanie tożsamością dla zaawansowanych
55	25.04.2024	Hewlett Packard Enterprise Polska sp. z o.o.	Centrum Operacji Bezpieczeństwa (SOC), nadzór i kontrola operacyjna w cyberbezpieczeństwie
56	09.05.2024	Krypton Polska sp. z o.o.	Ciągłość działania, ciągłość świadczenia, ciągłość bezpieczeństwa, jak zacząć.
57	16.05.2024	Axence, Polski Klaster Cyberbezpieczeństwa CyberMadeInPoland sp. z o.o.	Dobre praktyki działu IT w perspektywie norm i procedur bezpieczeństwa (NIS2, ISO27001)
58	23.05.2024	DAGMA SP. Z O.O.	OSINT: W sieci znajdziesz wszystko – poznaj tajniki Białego Wywiadu
59	13.06.2024	DEKRA Certification, Polski Klaster Cyberbezpieczeństwa CyberMadeInPoland sp. z o.o.	Zarządzanie incydentami bezpieczeństwa w dyrektywie NIS 2
60	20.06.2024	Elproma Elektronika sp. z o.o.	Desynchronizacja OT/IT infrastruktury krytycznej z użyciem JAMMINGU/SPOOFING GPS. Jak monitorować i zapobiegać.
61	27.06.2024	Net Complex, Polski Klaster Cyberbezpieczeństwa CyberMadeInPoland sp. z o.o.	Zarządzanie hasłami i kontrolą dostępu – wprowadzenie do systemu PAM
62	03.10.2024	Dynacon sp. z o.o.	Najważniejsze aspekty związane z materializacją i przeciwdziałaniem źródeł ryzyk w środowiskach przemysłowych
63	10.10.2024	SNOK Sp.z.o.o	Wprowadzenie do bezpieczeństwa systemów SAP

Tematy szkoleń – szkolenia dla operatorów usług kluczowych

EDYCJA 2021			
Lp.	**Data**	**Partner**	**Temat**
64	23.11.2021	Cisco International Limited	Rozpoznawanie i monitorowanie urządzeń w sieciach OT (300)
65	07.12.2021	Cisco International Limited	Segmentacja sieci przemysłowych (300)

EDYCJA 2022			
Lp.	**Data**	**Partner**	**Temat**
66	11.01.2022	Cisco International Limited	Wykrywanie podatności w sieciach przemysłowych (300)
67	22.02.2022	Dynacon sp. z o.o.	Fundamenty bezpieczeństwa usług kluczowych w środowiskach cyfrowych (300)

Tematy szkoleń dla podmiotów wykonujących działalność leczniczą

EDYCJA 2023			
Lp.	**Data**	**Partner**	**Temat**
68	16.10.2023	Cisco International Limited	Otoczenie prawne, wymagania i rekomendacje dla podmiotów świadczących usługi z zakresu ochrony zdrowia (inauguracja nowego cyklu)
69	14.11.2023	Cisco International Limited	Zero trust w placówkach ochrony zdrowia
70	13.12.2023	Cisco International Limited	Ochrona DNS – szybka i efektywna metoda ochrony przed zagrożeniami

EDYCJA 2024			
Lp.	**Data**	**Partner**	**Temat**
71	20.02.2024	Cisco International Limited	Segmentacja i kontrola dostępu do zasobów systemów szpitalnych
72	20.03.2024	Cisco International Limited	Bezpieczeństwo w sieciach bezprzewodowych Wireless LAN
73	16.04.2024	Cisco International Limited	Ochrona stacji końcowych przed cyberzagrożeniami
74	08.05.2024	Cisco International Limited	Bezpieczna komunikacja do internetu i usług chmurowych
75	21.05.2024	Cisco International Limited	Dlaczego należy dbać o bezpieczeństwo poczty elektronicznej
76	11.06.2024	Cisco International Limited	Uwierzytelnianie wieloskładnikowe (MFA) jako dodatkowa warstwa ochrony przed phishingiem i atakami opartymi o socjotechnikę
77	02.07.2024	Cisco International Limited	Identyfikacja i reagowanie na podatności w systemach IT

Sylwetki partnerów

Akamai Technologies to światowy lider w dziedzinie dostarczania treści, cyberbezpieczeństwa i rozwiązań chmurowych, który od ponad 26 lat wspiera firmy na całym świecie w tworzeniu bezpiecznych i niezawodnych doświadczeń cyfrowych. Dzięki globalnej sieci ponad 350 000 serwerów w 131 krajach przez Akamai przechodzi ponad 30% światowego internetu co daje nieporównywalną z niczym skalę. Akamai przyspiesza działanie stron internetowych i aplikacji, gwarantując użytkownikom maksymalną wydajność oraz bezpieczeństwo, niezależnie od ich lokalizacji. Dzięki ciągłemu monitorowaniu i analizie ruchu sieciowego, Akamai jest w stanie skutecznie identyfikować i odpierać zagrożenia cybernetyczne 24/7 zapewniając bezpieczeństwo danych swoim klientom. Firma jest pionierem w zakresie ochrony przed cyberzagrożeniami jak ataki DDoS, zarządzanie ryzykiem związanym z botami oraz zabezpieczenie przed cyberzagrożeniami. W portfolio Akamai znajdują się m.in. rozwiązania WAF, Zero Trust, API Security czy anty DDoS a firma ciągle rozbudowuje je tak, aby zapewnić holistyczne podejście do cyberbezpieczeństwa. Dla klientów w Polsce kluczową rolę odgrywa fakt, że w Krakowie znajduje się największy w Europie oddział Akamai, zatrudniający ponad 1000 inżynierów, a także zespoły SOCC i NOCC, które działają 24/7/365.

Amazon Web Services (AWS) jest wiodącym dostawcą chmury obliczeniowej, oferującym szeroką gamę usług w zakresie przetwarzania w chmurze dla firm, instytucji rządowych i klientów indywidualnych. Firma AWS należy do koncernu Amazon i została założona w 2006 roku. Dzięki AWS organizacje mogą szybko uzyskać dostęp do zasobów obliczeniowych, przechowywania danych, sieci oraz innych usług chmurowych bez konieczności inwestowania w kosztowną infrastrukturę IT. AWS oferuje ponad 200 w pełni skalowanych usług, w tym moc obliczeniowa, przechowywanie danych, bazy danych, analitykę, sztuczną inteligencję, uczenie maszynowe, Internet Rzeczy (IoT) i wiele innych. Platforma AWS jest wysoce niezawodna, bezpieczna i globalna. Jest obecna w 34 regionach geograficznych na całym świecie. Od wielu lat firma działa także w Polsce, gdzie powstała tzw. strefa lokalna AWS czyli rodzaj infrastruktury, w którym usługi AWS, takie jak np. moc obliczeniowa, pamięć masowa, bazy danych czy usługi kontenerowe znajdują się bliżej lokalnych klientów, umożliwiając wdrażanie aplikacji, które wymagają minimalnych opóźnień. AWS nieustannie wprowadza innowacje, pomagając firmom zwiększyć wydajność, obniżyć koszty i lepiej obsługiwać klientów.

anzena.
BEZPIECZEŃSTWO IT/OT

Anzena to dostawca i integrator informatyki przemysłowej. Współpracujemy z największymi polskimi przedsiębiorstwami, dla których tworzymy cyberbezpieczeństwo. Wdrażamy oraz integrujemy normy i dobre praktyki z architekturą Klienta. Edukujemy i budujemy cyberkompetencje IT/OT zakładów produkcyjnych, administracji publicznej i samorządowej. Jako firma integratorska, od 2012 roku zapewniamy przedsiębiorstwom aktywne wsparcie w utrzymaniu niezawodności systemów IT/OT.

Specjalizujemy się w audytowaniu sieci IT/OT, doradztwie i consultingu w obszarze procedur, polityk bezpieczeństwa, norm i standardów, oferujemy usługi inżynierskie. Zajmujemy się segmentacją i mikrosegmentacją sieci, bezpieczeństwem danych, budową i hardeningiem infrastruktury.

Anzena to zespół doświadczonych inżynierów IT/OT oraz architektów cyberbezpieczeństwa. Jesteśmy członkiem FAIRP Polska oraz Klastra Silesia Automotive & Advanced Manufacturing.

Anzena digitalizuje przemysł. Poznaj nas bliżej: www.anzena.eu

CISCO™

Cisco to światowy lider w dziedzinie bezpiecznych technologii tworzących Internet, które optymalizują działanie aplikacji, chronią dane, przekształcają infrastrukturę IT oraz łączą firmy i instytucje na całym świecie.

Zatrudniamy obecnie 80 tys. pracowników w 95 krajach, w tym prawie 3 tys. w trzech lokalizacjach w Polsce: Warszawie, Gdańsku i Krakowie. Nasze biuro w Krakowie to największe centrum zaawansowanych usług technicznych i biznesowych Cisco w regionie EMEA ze szczególnym naciskiem na cyberbezpieczeństwo.

Stale inwestujemy w Polsce, tworząc wysokiej jakości miejsca pracy w obszarze biznesu i technologii oraz wspierając realizację cyfrowej agendy naszego kraju w ramach Programu Cisco Country Digital Acceleration, którego jednym z filarów jest ochrona cyberbezpieczeństwa państwa.

Z kolei w ramach Programu Cisco Networking Academy co roku szkolimy w Polsce dziesiątki tysięcy uczniów i studentów w zakresie umiejętności cyfrowych, m.in. w obszarze cyberbezpieczeństwa. Od 2019 r. jesteśmy też aktywnymczłonkiem PWCyber.

Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland to organizacja branżowa zrzeszająca polskie firmy oferujące rozwiązania z zakresu cyberbezpieczeństwa. Klaster służy jako platforma współpracy, promocji oraz rozwoju polskiego przemysłu cyberbezpieczeństwa.

Klaster stymuluje także współpracę sektora prywatnego z instytucjami naukowymi, podmiotami administracji publicznej, międzynarodowymi korporacjami, izbami branżowymi i handlowymi, oraz innymi partnerami.

Organizujemy wydarzenia networkingowe, pomagamy nawiązywać relację biznesowe, a także wspieramy polskie firmy w ekspansji zagranicznej poprzez organizację misji handlowych czy udziału w wydarzeniach branżowych.

Klaster działa również aktywnie na polu edukacji rynku, poprzez autorskie cykle #CyberMadeInPoland Acedemy oraz w ramach porozumienia PWCyber, gdzie szkolimy z obszaru regulacji, trendów czy technologii.

Jesteśmy również członkiem Europejskiej Organizacji Cyberbezpieczeństwa (ECSO).

DAGMA Bezpieczeństwo IT to firma z niemal 40-letnią tradycją. Specjalizujemy się w rozwiązaniach i usługach z zakresu cyberbezpieczeństwa. Współpracujemy z kilkoma tysiącami Partnerów, zapewniając skuteczną ochronę IT ponad 8 mln klientów w Polsce oraz w Niemczech.

Audytujemy i doradzamy w kwestiach cyberbezpieczeństwa, pomagając wybrać najskuteczniejsze zabezpieczenia. Szkolimy ekspertów IT, a także oferujemy zaawansowaną usługę Secyrity Operations Center (SOC). Pomagamy również wdrożyć wybrane zabezpieczenia w docelowych infrastrukturach sieciowych klientów.

Wiemy, że wiarygodność w dziedzinie cyberbezpieczeństwa jest kluczowa, dlatego działamy zgodnie z rygorystycznymi normami ISO 27001 (System Zarządzania Bezpieczeństwem Informacji), ISO 22301 (System Zarządzania Ciągłością Działania), ISO 9001:2015 (System Zarządzania Jakością) oraz Wewnętrznym System Kontroli.

Dell Technologies oferuje kompleksowe rozwiązania w zakresie cyberbezpieczeństwa, bazujące na strategii Zero Trust, zgodnie z którą każdy dostęp do danych musi być zweryfikowany i monitorowany. Dzięki temu firmy mogą skutecznie chronić się przed zagrożeniami, takimi jak phishing czy ataki ransomware, które coraz częściej wykorzystują zaawansowane techniki do przenikania przez tradycyjne zabezpieczenia. Integralną częścią strategii Zero Trust jest cyfrowy bunkier, bezpieczne, odizolowane repozytorium kluczowych danych i systemów biznesowych, pozwalające na przechowywanie najważniejszych informacji w sposób niezależny od głównej sieci. Dzięki temu nawet w przypadku wycieku lub utraty danych najważniejsze zasoby pozostają chronione i mogą być szybko odzyskane. Cyfrowy Bunkier pomaga firmom nie tylko zapobiegać atakom, ale także sprawnie reagować na incydenty, minimalizując ich skutki i zapewniając ciągłość działania biznesu.

DYNACON Sp. z o. o. to polski producent rozwiązań komunikacji sieciowej i cyberbezpieczeństwa. Specjalizuje się w rynku i środowisku przemysłowym, a w szczególności dla sektorów: energetycznego, chemicznego, paliwowego, transportu, zaopatrzenia w wodę pitną i jej dystrybucję, ochrony zdrowia, przemysłu spożywczego i infrastruktury cyfrowej. Firma oferuje rozwiązania specjalnie zaprojektowane do zarządzania i zabezpieczania sieci komunikacyjnych przemysłowych systemów sterowania i środowiska AKPiA (Aparatura Kontrolno-Pomiarowa i Automatyka). Produkty DYNACON są również chętnie wykorzystywane w środowiskach IT. ARIC NDS Optical Industry Data Diode - Dioda Danych firmy DYNACON to pierwsza certyfikowana Dioda Danych w Europie. Posiada prestiżowy, międzynarodowy certyfikat CC L3 (norma Common Criteria), który udowadnia najwyższy poziom bezpieczeństwa, jaki zapewnia to rozwiązanie.

Od 2016 roku produkty Dynacon trafiły do ponad 100 podmiotów Infrastruktury Krytycznej Kraju, zapewniając komunikację i bezpieczeństwo dziedzinowym systemom OT.

Misją DYNACON od początku działalności jest rozwój polskiej myśli technologicznej, partnerstwo międzynarodowe, współtworzenie najlepszych praktyk w cyberbezpieczeństwie przemysłowym. DYNACON jako jedna z dziesięciu firm na kontynencie, została uhonorowana tytułem najlepszego dostawcy rozwiązań w zakresie cyberbezpieczeństwa w 2023 i 2024 roku.

Elproma to polska firma, która od ponad 30 lat prężnie rozwija się w sektorze ICT, produkując:

- Urządzenia telemetryczne (modemy i routery przemysłowe) dla energetyki, urządzeń medycznych, telekomunikacji, smart-city.
- Systemy synchronizacji czasu (serwery czasu NTP), systemy anty jamming/spoofing GPS/GNNS dla infrastruktur krytycznych m.in.: energetyki, wydobyciu surowców, produkcji paliw, wody, telecomów, bankowość, itp.

W Polsce Elproma zrealizowała m.in.: razem z Głównym Urzędem Miar projekt eCzasPL (wzorzec czasu dla Polski). To czwarte tego typu rozwiązanie na Świecie do wykorzystania przez wszystkie infrastruktury krytyczne, organizacje rządowe oraz podmioty komercyjne.

Elproma wyposaża w swoje systemy banki, Polską Agencję Żeglugi Powietrznej, sektor energetyczny i wiele innych. Elproma obecna na większości rynków Świata. Przykładem mogą być Filipiny, których system przesyłu energii chroniony jest przez Elproma.

Wg Elproma, synchronizacja czasu to fundament cyberbezpieczeństwa.

Engave S.A. od ponad 14 lat z pasją wspiera rozwój firm i instytucji w Polsce, pomagając im w pełni wykorzystać potencjał technologii. Wierzymy, że cyfryzacja nie jest celem samym w sobie, ale potężnym narzędziem, które realnie przekształca sposób działania organizacji. Rozumiemy, że każda firma jest unikalna, dlatego naszą pracę rozpoczynamy od dokładnego poznania jej celów, kultury pracy oraz wyzwań, przed którymi stoi.

Uważamy, że technologia powinna ułatwiać życie, a nie je komplikować, dlatego dostarczamy rozwiązania IT, które są nie tylko nowoczesne, ale przede wszystkim praktyczne i dostosowane do indywidualnych potrzeb naszych klientów.

Z myślą o rosnącym znaczeniu bezpieczeństwa danych, wyspecjalizowaliśmy się w cyberbezpieczeństwie i wdrożyliśmy jeden z największych Bunkrów Cyfrowych w Polsce, który chroni przedsiębiorstwa i instytucje publiczne przed zagrożeniami ransomware, pozwalając im działać bez zakłóceń, nawet w najtrudniejszych sytuacjach.

Naszym priorytetem jest, aby każda współpracująca z nami firma mogła bez obaw skupić się na swoim biznesie, mając pewność, że dbamy o niezawodność i bezpieczeństwo jej infrastruktury cyfrowej.

Ericsson jest dostawcą usług i serwisów dla operatorów telekomunikacyjnych, z 120-letnią obecnością na polskim rynku. W skład produktów firmy wchodzą infrastruktura sieci stałych i mobilnych, internet szerokopasmowy, rozwiązania IoT oraz tworzenie i utrzymanie aplikacji IoT, które stanowią fundament cyfrowej transformacji kraju.

Ericsson jest pionierem i aktywnym promotorem rozwiązań 5G w Polsce – wdrożył pierwszą komercyjną sieć 5G w Polsce z firmą Polkomtel, 5G w sieci Play, sieć testową w Warszawie z Orange oraz kampus 5G na Politechnice Łódzkiej.

Ericsson w Polsce ściśle współpracuje z operatorami telekomunikacyjnymi, sektorem publicznym i przemysłowym, wspierając rozwój innowacyjnych usług i aplikacji, które podnoszą jakość życia i konkurencyjność gospodarki.

Nasze centra badawczo-rozwojowe w Krakowie i Łodzi są zaangażowane w prace nad najnowszymi technologiami, z naciskiem na rozwój oprogramowania, sieci 5G i cyberbezpieczeństwo. Jako odpowiedzialny partner społeczny, Ericsson inwestuje w rozwój kompetencji cyfrowych, współpracując ze środowiskiem akademickim i i organizacjami edukacyjnymi na terenie całego kraju.

Grupa Euvic jest jedną z największych technologicznych grup kapitałowych na polskim rynku. Od 18 lat konsekwentnie poszerza zakres i kompleksowość swoich usług, opierając swoją działalność na sześciu filarach biznesowych: rozwój oprogramowania, infrastruktura IT, body/team leasing, innowacje, digital performance i konsulting. Główną przewagą konkurencyjną Euvic jest działanie w modelu 360°, zapewniające dostęp do kompetencji i usług w każdym obszarze IT, w tym rozwiązań z zakresu cyberbezpieczeństwa oraz wspierających cyfrową transformację biznesową klientów w Polsce i na świecie.

Evercom jest renomowanym dostawcą systemów teleinformatycznych, obecnym na rynku od 1992 roku. Dostarcza kompleksowe rozwiązania IT oraz świadczy zaawansowane usługi informatyczne.

Jest liderem w obszarze technologii bezpieczeństwa systemów i informacji. Evercom koncentruje się na obszarach kompetencyjnych: budowy centrów danych i sieci teleinformatycznych, systemów bezpieczeństwa, zarządzania infrastrukturą i usługami systemów IT, zunifikowanych systemów pamięci masowych, składowania danych oraz zarządzania procesami biznesowymi.

Evercom wykonuje audyty bezpieczeństwa informacji oraz systemów informatycznych.

Evercom jest zaangażowany w niekomercyjne projekty transformacji cyfrowej. Jednym z priorytetowych celów działania firmy, jest zapewnianie cyberbezpieczeństwa Rzeczpospolitej Polskiej jako niezbędnego elementu naszej suwerenności. W ramach Programu Współpracy w Cyberbezpieczeństwie (PWCyber), Evercom dzieli się doświadczeniami z instytucjami publicznymi.

Fortinet to globalny dostawca rozwiązań z zakresu cyberbezpieczeństwa. Misją firmy jest zabezpieczanie ludzi, urządzeń i danych na całym świecie. Firma specjalizuje się w dostarczaniu kompleksowych, zintegrowanych systemów ochrony sieci i pomaga reagować na stale zmieniający się krajobraz cyberzagrożeń. Współpraca z organizacjami zarówno z sektora publicznego, jak i prywatnego, w tym CERT-ów (z różnych krajów), jednostkami rządowymi i środowiskiem akademickim,to kluczowy element zaangażowania Fortinet w zwiększanie odporności na zagrożenia w cyberprzestrzeni.

Instytut szkoleniowy Fortinet oferuje jeden z największych i najszerszych programów szkoleniowych w branży, którego celem jest udostępnianie wszystkim zainteresowanym szkoleń z zakresu cyberbezpieczeństwa i nowych możliwości kariery. FortiGuard Labs, elitarna organizacja Fortinet zajmująca się analizą zagrożeń i badaniami nad nimi, wykorzystuje wiodące technologie uczenia maszynowego i sztucznej inteligencji, aby zapewnić klientom niezmiennie najwyższej jakości ochronę i przydatne informacje o zagrożeniach.

Więcej informacji o działalności Fortinet można uzyskać na stronie internetowej: https://www.fortinet.com/

Fudo Security to globalny lider w zarządzaniu uprzywilejowanym dostępem, oferujący nowatorskie rozwiązania zapewniające bezpieczny dostęp zdalny. Nasze produkty, dedykowane firmom każdej wielkości i branży, umożliwiają monitorowanie działań użytkowników, ochronę przed nieuprawnionym dostępem oraz skuteczne zarządzanie dostępem do kluczowych zasobów. Dzięki nam organizacje nie tylko zapobiegają zagrożeniom, ale także szybko i efektywnie na nie reagują. Od 2004 roku wspieramy klientów w ponad 30 krajach na całym świecie.

Fudo Security wyróżnia się zaawansowanym monitoringiem sesji, analizą behawioralną wspieraną przez AI oraz błyskawicznym wdrożeniem w jeden dzień. Flagowe produkty Fudo Enterprise i Fudo One odpowiadają na potrzeby współczesnych firm, oferując Secure Third Party Access i Intelligent NextGen PAM. Nasze innowacje zdobyły globalne uznanie, w tym nagrody Cybersecurity Excellence Award i Kuppingercol Innovation Leader.

Fundacja Bezpieczna Cyberprzestrzeń to niezależna organizacja pozarządowa, działająca od 2010 roku, której celem jest działanie na rzecz bezpieczeństwa cyberprzestrzeni. Realizowane jest to przez działalność w trzech głównych obszarach: uświadamiania o zagrożeniach teleinformatycznych, monitorowania zjawisk i przypadków związanych z naruszaniem bezpieczeństwa w cyberprzestrzeni, prowadzenia działalności badawczo-rozwojowej. Posiadamy bogate doświadczenie w organizacji ćwiczeń cyberbezpieczeństwa, realizowanych w ramach projektu Cyber-EXE Polska®, które zwiększają zdolności organizacji i struktur państwowych do ochrony przed cyberatakami. Stworzyliśmy również platformę edukacyjną CyberBastion®, która uczy budowania struktur cyberbezpieczeństwa i reagowania na ataki. Od 2014 roku organizujemy konferencję SECURITY CASE STUDY, koncentrującą się na technicznych aspektach cyberbezpieczeństwa i analizie studiów przypadków. Eksperci Fundacji są wykładowcami na wielu uczelniach wyższych oraz autorami licznych ekspertyz.

Google Polska to znacznie więcej niż tylko wyszukiwarka. To firma obecna w Polsce od 2005 roku, zatrudniająca ponad 1700 osób i generująca ponad 6500 dodatkowych miejsc pracy w firmach współpracujących. Oprócz wyszukiwarki, Google oferuje szereg usług używanych na co dzień przez miliony Polaków, np. Mapy, YouTube, Android i chmurę obliczeniową, która jest rozwijana w warszawskim Google Cloud Development Center - największym centrum rozwoju technologii Google Cloud w Europie. Google wykorzystuje sztuczną inteligencję do ulepszania swoich produktów i usług, aby były one jeszcze bardziej pomocne i użyteczne dla ludzi na całym świecie.

Google wspiera rozwój polskich firm poprzez szkolenia i programy, z których skorzystało ponad 100 000 przedsiębiorstw. Google for Startups Campus w Warszawie stworzył ekosystem 1800 firm, generując 6500 miejsc pracy i pozyskując 480 mln dolarów finansowania.

Wszystkie usługi Google są oparte na najnowocześniejszych zabezpieczeniach, chroniąc więcej osób online niż ktokolwiek inny na świecie. Google aktywnie buduje bezpieczniejszy internet dla wszystkich Polaków organizując warsztaty i szkolenia, które podnoszą świadomość o zagrożeniach w sieci, a także współpracuje z instytucjami rządowymi i organizacjami pozarządowymi, chroniąc je przed zagrożeniami.

Google jest zaangażowanym inwestorem w Polsce. Inwestujemy tutaj, ponieważ wierzymy, że Polska ma potencjał, aby stale umacniać swoją pozycję jako lider technologiczny w regionie.

Galach Consulting świadczy kompleksowe usługi z zakresu cyberbezpieczeństwa i zarządzania bezpieczeństwem informacji. Pomagamy naszym klientom chronić ich aktywa informacyjne – skutecznie, zgodnie z wymaganiami prawnymi, regulacyjnymi, biznesowymi i zdrowym rozsądkiem.

Nasze usługi obejmują zarówno ocenę bezpieczeństwa organizacji jak i działania pozwalające na jej dostosowanie do wymagań normatywnych i regulacyjnych. Wdrażamy systemy zarządzania bezpieczeństwem informacji zgodne z ISO/IEC 27001 oraz systemy zarządzania ciągłością działania zgodne z ISO 22301. Przeprowadzamy również analizy i testy bezpieczeństwa systemów informatycznych, pozwalające na zidentyfikowanie i oszacowanie podatności oraz wskazania możliwości ich racjonalnego usunięcia.

Współpracując z wiodącymi centrami szkoleniowymi w kraju i zagranicą prowadzimy specjalistyczne szkolenia z zakresu zarządzania bezpieczeństwem, w tym przygotowujące do egzaminu CISSP.

HackingDept od 2018 roku tworzy nowoczesną, polską platformę szkoleniową – zaawansowany cyber poligon nowej generacji.

Platforma umożliwia naukę poprzez symulację ataków na zróżnicowane środowiska, wprowadzając uczestników w świat technik ofensywnych oraz metod obrony przed nimi. Celem tego cyber poligonu jest pogłębienie praktycznych umiejętności specjalistów, zwłaszcza tych pracujących z infrastrukturą krytyczną, co umożliwia lepsze zrozumienie i adaptację do stale ewoluujących, rzeczywistych metod ataków występujących w środowiskach teleinformatycznych.

Zespół HackingDept to doświadczeni inżynierowie bezpieczeństwa IT i programiści, członkowie najbardziej utytułowanych polskich zespołów zajmujących się drużynowym przełamywaniem zabezpieczeń – Dragon Sector i p4. Jako medaliści dziesiątek międzynarodowych konkursów hakerskich typu Capture The Flag, w latach 2018-2019 znajdowali się na podium globalnego rankingu. W ostatnich latach drużyny te próbowały swoich sił w bezpieczeństwie technologii kosmicznych, czterokrotnie stając na podium finałów międzynarodowych zawodów Hack-A-Sat, organizowanych przez Defense Digital Service, U.S. Space Force oraz U.S. Air Force.

Hewlett Packard Enterprise to globalny dostawca rozwiązań technologicznych obejmujących zakres od brzegu sieci aż po chmurę obliczeniową, które pomagają organizacjom szybciej osiągać zamierzone efekty, dzięki odblokowaniu potencjału drzemiącego w gromadzonych przez nie danych. Wieloletnia historia innowacji, które zmieniają na lepsze sposób, w jaki żyjemy i pracujemy, umożliwia HPE oferowanie unikalnych, otwartych i inteligentnych rozwiązań, udostępnianych w modelu usługowym. Portfolio HPE obejmuje usługi chmurowe, rozwiązania obliczeniowe, wysokowydajną infrastrukturę obliczeniową (HPC) i sztuczną inteligencję, Intelligent Edge, a także oprogramowanie i pamięć masową. Dzięki swoim usługom firma pomaga partnerom w opracowywaniu nowych modeli biznesowych, nowych sposobów angażowania klientów i w zwiększaniu wydajności operacyjnej. Więcej informacji można znaleźć na stronie: www.hpe.com.

IBM jest wiodącym dostawcą rozwiązań chmury hybrydowej i sztucznej inteligencji oraz usług konsultingowych. Pomagamy klientom w ponad 175 krajach wykorzystywać wgląd w dane, usprawniać procesy biznesowe, obniżać koszty i zdobywać przewagę konkurencyjną w swoich branżach. Ponad 4000 podmiotów rządowych i korporacyjnych w krytycznych obszarach infrastruktury, takich jak usługi finansowe, telekomunikacja i opieka zdrowotna, polega na platformie chmury hybrydowej IBM i Red Hat OpenShift, aby szybko, wydajnie i bezpiecznie wpływać na ich transformacje cyfrowe. Przełomowe innowacje IBM w zakresie sztucznej inteligencji, obliczeń kwantowych, dedykowanych rozwiązań chmurowych i doradztwa zapewniają naszym klientom otwarte i elastyczne opcje. Wszystko to jest wspierane przez wieloletnie zaangażowanie IBM w zaufanie, przejrzystość, odpowiedzialność, integrację i obsługę.

Na polskim rynku IBM działa od ponad 30 lat. Poza główną siedzibą firmy w Warszawie, posiada również szereg specjalistycznych centrów, takich jak Centrum Usług Finansowo-Księgowych i Laboratorium Oprogramowania IBM w Krakowie oraz IBM X-Force Command Center we Wrocławiu.

ICsec S.A. to dostawca rozwiązań z zakresu cyberbezpieczeństwa dedykowanych dla przemysłu, w tym infrastruktury krytycznej. Opracowana przez ICsec platforma SCADvance XP® adresuje potrzeby związane z monitoringiem sieci automatyki przemysłowej, wykrywaniem potencjalnych zagrożeń i anomalii w ruchu pomiędzy podłączonymi do sieci urządzeniami.

W erze cyfrowego wyścigu zbrojeń kwestią kluczową pozostaje szybkość reakcji. Systemy potrafiące adaptować się do detekcji nowych zagrożeń mają znaczącą przewagę nad tradycyjnymi systemami. Platforma SCADvance XP® dostarczana przez ICsec tworzy modele dostosowane do specyficznych charakterystyk chronionych sieci, obejmując szeroki zakres potencjalnych zagrożeń. Dzięki temu skutecznie uzupełnia tradycyjne metody wykrywania, takie jak metody oparte na regułach i sygnaturach, które koncentrują się na znanych zagrożeniach.

Rozwiązania ICsec pozwalają na znaczące zmniejszenie ryzyka biznesowego związanego z cyberatakami na sieci przemysłowe, skutecznie wspierając wiodące polskie przedsiębiorstwa w zabezpieczaniu ich infrastruktury.

Immunity Systems jest polską firmą zajmująca się pełnym spektrum zagadnień związanych z bezpieczeństwem IT. Nasz zakres usług obejmuje szeroki wachlarz działań związanych z cyberbezpieczeństwem.

Dużym atutem naszej firmy jest zespół ekspertów, który posiada wieloletnie doświadczenie, gwarantujące najwyższy poziom bezpieczeństwa informatycznego, zarówno ofensywnego i defensywnego.

Do głównych specjalizacji firmy należą:

- Badanie systemów krytycznych dla bezpieczeństwa klienta np. system autoryzacji użytkowników,
- Badanie systemów zabezpieczających nietypowe organizacje oraz procesy np. infrastrukturę honeypot symulującą prawdziwą infrastrukturę klienta,
- Analizy pod kątem bezpieczeństwa rozwiązań IT, systemów automatyki przemysłowej oraz urządzeń embedded
- Symulację ataku cyberprzestępcy,
- Prace badawczo-rozwojowe związane z produktami bezpieczeństwa IT np. wybór najlepszego rozwiązania w kontekście już istniejącej infrastruktury klienta,
- Wsparcie przy analizie złożonych technicznie incydentów bezpieczeństwa
- Inżynieria odwrotna oprogramowania np. programu malware, który zaatakował klienta.

Integrated Solutions należy do grona największych integratorów technologicznych w Polsce. Firma specjalizuje się w projektowaniu i dostarczaniu zaawansowanych usług ICT dla biznesu, instytucji publicznych i służb mundurowych. Realizuje projekty w zakresie bezpieczeństwa, infrastruktury IT, chmury, rozwiązań Microsoft i szeroko rozumianej cyfrowej transformacji. Jej działania są odpowiedzią na rosnące zapotrzebowanie klientów na spójne, kompleksowe zarządzanie infrastrukturą teleinformatyczną. Produkty i usługi spółki są oparte na najwyższych standardach i partnerstwach technologicznych ze światowymi liderami rynku. Firma stale rozwija swoje kompetencje w domenie bezpieczeństwa cyfrowego - tworzy rozwiązania, które łączą najnowocześniejsze technologie cyberbezpieczeństwa z ekspercko zaprojektowanymi i sprawdzonymi procesami oraz dobrymi praktykami w obszarze ochrony danych. Jest jednym z największych w kraju dostawców rozwiązań z tego obszaru (6 miejsce wg Raportu Best100 ITWIZ).

W portfolio Integrated Solutions znajduje się ponad 500 Klientów z sektora publicznego i prywatnego.

Krypton Polska od 20 lat zapewnia skuteczną ochronę informacji niejawnych i wrażliwych w cyfrowym świecie, budując szyfratory nowej generacji i wspierając kryptograficzną ekspertyzą kluczowe organizacje państwowe. Produkty Krypton cechują się wysokimi parametrami pracy, łatwością obsługi i najwyższymi standardami bezpieczeństwa, potwierdzonymi certyfikatami Agencji Bezpieczeństwa Wewnętrznego i Służby Kontrwywiadu Wewnętrznego. Misją Krypton Polska jest również budowanie długoletnich relacji biznesowych opartych na szacunku i etyce oraz wspieranie inicjatyw zwiększających bezpieczeństwo Polski w cyfrowym świecie, takich jak PWCyber. Jesteśmy dumni, że Krypton jest pierwszą polską firmą, która dołączyła do tego Programu. – Michał Czmoch, Prezes Zarządu.

Mediarecovery to lider informatyki śledczej wspierający służby oraz klientów biznesowych w walce z cyberprzestępczością i nadużyciami.

Dostarczamy rozwiązania pomagające pozyskiwać dowody cyfrowe, przyspieszać rozwiązywanie prowadzonych śledztw oraz ułatwiać procesy decyzyjne, a także chronić organizacje przed cyberatakami.

W naszej ofercie znajdziesz:

- Dystrybucję wiodących na świecie narzędzi digital forensics.
- Usługi prowadzone w ramach największego w Polsce Laboratorium Informatyki Śledczej.
- Projektowanie i budowę laboratoriów informatyki śledczej.
- Usługę CSIRT as a Service - monitorowanie środowiska informatycznego i reakcji na incydenty bezpieczeństwa.
- Projektowanie i budowę specjalistycznej zabudowy pojazdów na potrzeby służb mundurowych.
- Działania edukacyjne, w tym Akademię Informatyki Śledczej Mediarecovery, która szkoli specjalistów informatyki śledczej.
- Największą konferencję informatyki śledczej po tej stronie Europy, zrzeszającą ekspertów z całego świata.

Microsoft jest uczestnikiem Programu PWCyber od 2023 roku. Jako inicjatywa skierowana do uczestników Krajowego Systemu Cyberbezpieczeństwa, PWCyber jest istotnym dopełnieniem Programu Microsoft Government Security Program (GSP), którego uczestnikami są wybrane agencje rządowe.

W dobie transformacji cyfrowej niezbędne są skuteczne działania na rzecz poprawy bezpieczeństwa w cyberprzestrzeni. Wymaga to kompleksowego podejścia uwzględniającego nie tylko kwestie techniczne, lecz również organizacyjne, a przede wszystkim czynnik ludzki. Świadomość znaczenia cyberhigieny ma tu fundamentalne znaczenie.

Z tego względu Microsoft intensywnie angażuje się w budowanie kompetencji kadr sektora publicznego oraz zapewnia dostęp do najnowszych rozwiązań i transfer specjalistycznej wiedzy do najlepszych zespołów w kraju. Dzięki PWCyber razem wzmacniamy odporność państwa i wspieramy jego rozwój, równocześnie realizując misję Microsoft – żeby każdy człowiek i każda organizacja mogła osiągnąć więcej.

Nokia jest wiodącym dostawcą rozwiązań telekomunikacyjnych, stanowiących fundament współczesnego świata. Oferując nowoczesne rozwiązania, łączy ze sobą miliardy ludzi i urządzeń.

W Nokii w Polsce jest zatrudnionych prawie siedem tysięcy osób, z czego znaczna większość w centrach R&D w czterech miastach: Wrocławiu, Krakowie, Warszawie i Bydgoszczy.

W polskich laboratoriach Nokii są projektowane i rozwijane najnowsze technologie, takie jak: LTE, 5G, Single RAN i Radio Cloud. Pracujemy nad technologiami telekomunikacyjnymi będącymi fundamentami globalnej łączności. Rozwijamy wszystkie technologie radiowe oraz posiadamy najnowszej generacji sprzęt do ich testowania.

W naszych centrach R&D każdego dnia są tworzone rozwiązania, które są używane na całym świecie.

Więcej o firmie: https://nokiawroclaw.pl/, https://nokia.com/
FB: https://www.facebook.com/NOKIAinPoland/

nomios

Nomios Poland działa na rynku od 2012 roku obsługując największe firmy z sektora finansowego, energetycznego, telekomunikacyjnego, sieci retailowe oraz instytucje publiczne.

Specjalizujemy się w projektowaniu, wdrażaniu, obsłudze i zarządzaniu rozwiązaniami cyberbezpieczeństwa, które umożliwiają klientom wprowadzanie innowacji, zapewniają wydajność, elastyczność i sprawność operacyjną. Tym, co wyróżnia naszą firmę, jest zespół przeszkolonych, zdolnych ludzi, skupionych na tym, aby świadczyć usługi na wyjątkowym poziomie.

Oferujemy usługi SOC i NOC w trybie 24/7 oraz autorski system do klasyfikacji dokumentów i poczty elektronicznej GREENmod. Posiadamy zdolność do kompleksowej obsługi i realizacji projektów niejawnych krajowych i zagranicznych, w ramach Świadectw Bezpieczeństwa Przemysłowego III stopnia. Uzyskaliśmy liczne certyfikacje takie jak ISO 22301, ISO 27001 oraz Trusted Introducer.

Współpracujemy z wiodącymi producentami technologicznymi, takimi jak Juniper Networks, Fortinet, Trellix, Infoblox i F5 Network. Dzięki naszemu bogatemu portfolio możemy sprostać nawet najbardziej wymagającym oczekiwaniom klientów.

ORACLE

Misją Oracle jest pomaganie ludziom postrzegać dane w nowy sposób, odkrywać informacje, odblokowywać nieskończone możliwości. Od ponad czterech dekad firma dostarcza innowacje, na których zbudowano całe branże. Oracle współpracuje w Polsce z kluczowymi instytucjami państwowymi, bankami, szpitalami i dużymi firmami prywatnymi.

Oracle to jedyny dostawca technologii, który oferuje kompletny pakiet zintegrowanych aplikacji chmurowych oraz chmurową platformę infrastrukturalną. Platforma Oracle Cloud udostępnia wszystkie usługi potrzebne do migracji, budowy i eksploatacji infrastruktury informatyczne, począwszy od istniejących procesów po nowe chmurowe aplikacje i platformy danych. Aplikacje Oracle zostały zbudowane na bazie infrastruktury chmurowej Oracle i obejmują moduły obsługi klienta i zaplecza pozwalające na obsługę spójnych procesów i pojedynczych źródeł danych w ramach najważniejszych funkcji biznesowych.

Orange Polska jest jednym z wiodących dostawców usług telekomunikacyjnych w kraju. Dzięki nowoczesnej infrastrukturze oferuje internet światłowodowy o szybkości nawet do 8 Gb/s oraz usługi mobilne w technologii 5G. Jest dostawcą kompleksowych rozwiązań dla biznesu, oferuje usługi z zakresu IoT, ICT i cyberbezpieczeństwa. Od ponad 25 lat dba o bezpieczeństwo internautów. Specjalistyczny zespół CERT Orange Polska nieustanie rozwija narzędzia pozwalające monitorować i blokować zagrożenia zanim dotrą do urządzeń klientów. Tylko w 2023 roku działająca w sieci Orange Polska CyberTarcza zablokowała ponad 360 tysięcy fałszywych stron internetowych i ochroniła około 5,5 mln użytkowników. Usługi Orange Polska pomagają użytkownikom osiągać zgodność z wymaganiami regulacyjnymi cyberbezpieczeństwa.

Operator wspiera też edukację cyfrową - poprzez programy Fundacji Orange uczy bezpiecznego i twórczego korzystania z nowoczesnych technologii.

Palo Alto Networks to amerykańska korporacja zajmująca się cyberbezpieczeństwem, założona w 2005 roku przez Nir Zuk. Firma ma swoją siedzibę w Santa Clara w Kalifornii i jest jednym z czołowych graczy na rynku oprogramowania i sprzętu związanego z bezpieczeństwem sieciowym. Jej produkty i usługi są wykorzystywane na całym świecie do ochrony systemów korporacyjnych, chmur, centrów danych i sieci IoT przed różnorodnymi zagrożeniami cybernetycznymi.

Palo Alto Networks nie ogranicza się jednak tylko do zapór sieciowych. Portfolio firmy obejmuje również produkty do ochrony endpointów, takie jak Traps, narzędzia do analizy i raportowania, jak Cortex, oraz rozwiązania do zabezpieczania chmur i kontenerów. Wszystko to jest integrowane w ramach platformy natywnej dla chmury, co umożliwia klientom bardziej spójne i efektywne zarządzanie bezpieczeństwem w różnorodnych środowiskach

Palo Alto Networks jest również aktywnym uczestnikiem społeczności zajmującej się cyberbezpieczeństwem. Firma sponsoruje badania, publikuje raporty o zagrożeniach i najlepszych praktykach, a także oferuje różne formy szkoleń i certyfikacji dla profesjonalistów w tej dziedzinie.

Perceptus Sp z o. o. od 2008 roku działa na rynku cyberbezpieczeństwa. Kompleksowo zabezpiecza ekosystem IT klientów, równolegle tworząc własne rozwiązania i oprogramowanie. Zajmuje się między innymi szyfrowaniem danych, ich backupem, archiwizacją i wirtualizacją, ale również integracją oprogramowania chroniącego urządzenia końcowe. W portfolio zrealizowanych projektów może pochwalić się największym w Europie wdrożeniem systemów endpoint protection, zabezpieczającym jednocześnie 85 000 urządzeń.

SOC Perceptus realizuje dla klientów usługi Security Operations Center, a procesy realizowane w tym obszarze są świadczone zgodnie ze standardem ISO 27001:2017.

Projekty własne opracowane i wdrożone przez Perceptus to m.in.: zaawansowany podpis elektroniczny zgodny z dyrektywą eIDAS, Mobilne Data Center wyposażone w pełną infrastrukturę informatyczną, które pozwala m. in. na bezpieczny backup z wykorzystaniem kluczy kryptograficznych czy pierwszy polski menedżer haseł perc.pass.

PKP Informatyka to główny dostawca usług IT w Grupie PKP. Tworzy i zapewnia ciągłość działania oraz bezpieczeństwo kluczowych dla kolei systemów i aplikacji.

PKP Informatyka wspiera transport kolejowy w jego cyfrowej transformacji, dostarczając stabilne i niezawodne rozwiązania IT. Usługi Spółki obejmują kompleksową obsługę informatyczną, od infrastruktury i bezpieczeństwa po aplikacje i wsparcie użytkowników.

Spółka świadczy usługi w zakresie tworzenia oprogramowania użytkowego – przede wszystkim przeznaczonego dla spółek Grupy PKP, eksploatacji bezpośredniej systemów i aplikacji, a także kolokacji, hostingu, serwisu sprzętu komputerowego, wykonawstwa sieci strukturalnych itp.

Spółka posiada nowoczesne, wyspecjalizowane zespoły Security Operations Center oraz Network Operations Center, które wraz z zespołem CERT PKP Informatyka przyczyniają się do wzrostu poziomu bezpieczeństwa IT w transporcie kolejowym, a także rozwoju Krajowego Systemu Cyberbezpieczeństwa. PKP Informatyka posiada bogate doświadczenie w doradztwie i wdrażaniu rozwiązań IT. Dzięki znajomości specyfiki branży oraz regulacji prawnych, dostarcza rozwiązania zgodne z obowiązującymi normami polskimi i unijnymi.

PROGET

Proget Sp. z o.o. to jedyny w pełni polski producent autorskiego rozwiązania klasy MDM/EMM, które zabezpiecza urządzenia mobilne w sektorze publicznym i prywatnym. Firma działa zgodnie z międzynarodowymi normami: zarządzania bezpieczeństwem informacji ISO/IEC 27001 i zarządzania jakością ISO 9001. Spółka jest członkiem rządowego porozumienia PWCyber oraz klastra Cyber Made in Poland. W swoich działaniach stawia na aktywne budowanie świadomości Cyberbezpieczeństwa, edukując na temat cyberzagrożeń i propagując dobre praktyki oraz zasady cyberhigieny.

System Proget to rozbudowane, w pełni konfigurowalne narzędzie do zdalnego zarządzania urządzeniami mobilnymi, kontroli aplikacji i ochrony danych przetwarzanych przez organizacje zgodnie z wymogami RODO oraz NIS2. Upraszcza zarządzanie różnymi systemami operacyjnymi (Android, iOS, iPadOS, macOS i Windows) zapewniając administratorom IT możliwość kontroli wszystkich zasobów z poziomu jednego interfejsu.

SAMSUNG

Współpraca Samsung Electronics Polska i Ministerstwa Cyfryzacji w ramach PWCyber – Programu Współpracy w Cyberbezpieczeństwie rozpoczęła się w 2019 roku. Samsung Polska przystąpił do Programu jako pierwszy sygnatariusz. W ramach współpracy w ekosystemie partnerów uczestniczymy w procesie podnoszenia kompetencji pracowników struktur administracji publicznej, wojska, edukacji i spółek skarbu państwa, uczelni wyższych poprzez prowadzenie szkoleń z cyberbezpieczeństwa i certyfikacji urządzeń (KSO3C – Common Criteria, SDIP, inne), przygotowywania rekomendacji i raportów branżowych.

Prowadzimy aktywne działania w zakresie identyfikacji zagrożeń i podatności cyberbezpieczeństwa w zakresie urządzeń mobilnych. Realizujemy również działania promocyjne za pośrednictwem publikacji naukowych, konferencji branżowych (np. Cyber Day, Defence Day).

Samsung w Polsce posiada jedno z największych na świecie centrów badawczo-rozwojowych zlokalizowanych w Warszawie. W ramach porozumienia dostarcza i tworzy rozwiązania poddane certyfikacji przez organy państwowe, takie jak m.in. ABW (i inne organizacje służb specjalnych odpowiedzialnych za bezpieczeństwo państwa) NASK, Instytut Łączności. Współpracujemy aktywnie z polskimi podmiotami w zakresie partnerstw biznesowych takimi jak m.in. Asseco Data System, Siltec, spółki z grupy WB Electronics.

SECAWA wspiera firmy w szacowaniu i minimalizowaniu ryzyk związanych z atakami socjotechnicznymi. Praktyczny Trening Antyphishingowy uczy pracowników rozpoznawać i reagować na phishing, zwiększając ich ostrożność i świadomość zagrożeń. Dedykowane, różnorodne symulacje odwzorowują realne ataki, a zdobyte doświadczenia i wiedza są dobrze zapamiętywane przez pracowników i zmieniają ich nawyki na bezpieczniejsze. Testy socjotechniczne skupiają się na wykryciu podatności pracowników na manipulacje socjotechniczne. Obie usługi są mierzalne i dostarczają szczegółowe statystyki pozwalające zidentyfikować wrażliwe obszary, oszacować ryzyko oraz ocenić skuteczność procedur w organizacji.

SECAWA zapewnia kompleksowe wsparcie: od analizy potrzeb, przez prowadzenie działań po ewaluację wyników rekomendacje, co umożliwia utrzymanie wysokiej intensywności i jakości usług przy minimalnym zaangażowaniu klienta.

Usługi SECAWA wpisują się w wytyczne wymagań NIS2, DORA, RODO, ISO 27001.

Esecure Sp. z o.o. to polski producent platformy SecureVisio, służącej do kompleksowego zarządzania bezpieczeństwem IT. Platforma daje możliwość wykrywania i zarządzania podatnościami oraz incydentami bezpieczeństwa, a także pozawala automatyzować i ujednolicać operacje związane z zarządzaniem bezpieczeństwem.

Jednocześnie poprzez dodanie kontekstu biznesowego do zabezpieczeń technicznych, SecureVisio poprawia elastyczność organizacji w zakresie ryzyka i odporność biznesową na cyberzagrożenia.

securitum

Securitum działa na rynku cyberbezpieczeństwa od 2009 roku realizujac autorskie, uznane na rynku projekty IT Sec.

Zespół Securitum Audyty, dysponujac największym w Polsce zespołem pentesterskim realizuje ponad 800 pentestów rocznie, w tym aplikacji, sieci oraz testów socjotechnicznych. Konsultanci Securitum badają bezpieczeństwo największych instytucji finansowych, firm z branży telekomunikacyjnej oraz usługowej, zarówno w kraju, jak i za granicą.

Securitum Szkolenia specjalizuje się w przeprowadzaniu szkoleń z zakresu bezpieczeństwa IT, zarówno dla osób technicznych jak i nietechnicznych. Flagowym projektem edukacyjnym spółki, wspieranym przez portal sekurak.pl jest Sekurak.Academy gromadzący unikalną w skali kraju społeczność IT Sec, liczącą ponad 10 tysięcy uczestników. Firma organizuje także uznaną na rynku konferencję Mega Sekurak Hacking Party.

Od 2019 roku nakładem Securitum Wydawnictwo ukazują się książki z zakresu bezpieczeństwa IT, każdorazowo osiągające imponujące nakłady wydawnicze.

SEVENET

SEVENET S.A. od ponad 25 lat dostarcza zaawansowane rozwiązania teleinformatyczne. Od czerwca 2011 r. akcje Spółki notowane są w Alternatywnym Systemie Obrotu rynku NewConnect. Spółka wykonuje prace dla jednych z największych polskich przedsiębiorstw oraz instytucji w Polsce. Swoją działalność opiera na czterech filarach: rozwiązaniach do współpracy i komunikacji biznesowej, dostępu do sieci, wyposażeniu centrów danych oraz cyberbezpieczeństwie. Posiadamy liczne certyfikaty ISO, WSK, które potwierdzają jakość świadczonych przez nas usług. Dodatkowo posiadamy świadectwa Bezpieczeństwa Przemysłowego UE oraz NATO III-go stopnia.

Rekomendujemy wszystkim współpracę w ramach Programu Współpracy w Cyberbezpieczeństwie (PWCyber). Sevenet S.A. od 2 lat aktywnie uczestniczy w tym przedsięwzięciu i dostrzega w nim ogromny potencjał do dalszego rozwoju.

Smartech-IT to firma specjalizująca się w rozwiązaniach z zakresu bezpieczeństwa informatycznego i zarządzania danymi. Nasz zespół certyfikowanych ekspertów zapewnia kompleksowe usługi, w tym audyty bezpieczeństwa informacji, wdrażanie systemów zarządzania bezpieczeństwem (ISO 27001, ISO 22301) oraz doradztwo w zakresie ochrony danych i cyberbezpieczeństwa. Dysponujemy także certyfikowanym przez niezależną firmę Centrum Bezpieczeństwa Cyfrowego (SOC), które stanowi kluczowy element naszej strategii ochrony i monitorowania środowiska IT klientów. Naszym celem jest wspieranie klientów w tworzeniu bezpiecznego środowiska IT, które spełnia najwyższe standardy bezpieczeństwa i zgodności z regulacjami. Dążymy do stałego rozwoju i wprowadzania innowacji, by skutecznie chronić dane naszych klientów.

SNOK jest wiodącym ekspertem w dziedzinie cyberbezpieczeństwa systemów SAP. Firma pełni rolę strategicznego partnera dla czołowych podmiotów branży IT, takich jak SAP, Microsoft, Lenovo, SuSE oraz SecurityBridge.

Specjalizacja SNOK obejmuje kompleksowe doradztwo w zakresie bezpieczeństwa, wdrożenia systemów SAP oraz analizę i minimalizację ryzyka cybernetycznego. Firma oferuje spersonalizowane rozwiązania zabezpieczające, dostosowane do indywidualnych potrzeb klientów.

Oferta firmy obejmuje m.in.:

- unikalne metodyki zabezpieczania systemów SAP
- profesjonalne usługi pentestingowe
- badania nad wykrywaniem nowych podatności
- dedykowany SOC (Security Operations Center) działający 24/7
- programy edukacyjne i szkolenia

Jako partner Programu PWCyber, SNOK przyczynia się do wzmacniania krajowego systemu cyberbezpieczeństwa. Wieloletnie doświadczenie w tym obszarze ma kluczowe znaczenie dla bezpieczeństwa danych w instytucjach publicznych.

StillSec to polska spółka, która istnieje od 2015 roku firma, świadcząca usługi w zakresie cyberbezpieczeństwa łączące obszar zapewnienia zgodności z wiedzy technicznej. Misją StillSec jest ochrona informacji będących własnością klientów, rozwój strategii i technik bezpieczeństwa informacji oraz budowanie kompetencji i świadomości w zakresie bezpieczeństwa. Spółka świadczy także usługi doradcze, które pozwalają organizacjom na dostosowanie do zmieniających się wymagań (takich jak NIS2, DORA, itp.), pozwalają na zwiększenie odporności na zakłócenia biznesowe i efektywne rozwiązywanie problemów związanych z bezpieczeństwem informacji. StillSec prowadzi audyty dostawców i wspiera organizacje w trakcie audytów realizowanych przez ich Klientów. Ponadto Spółka posiada własne centrum monitorowania (SOC) i zespół reagowania na incydenty komputerowe (CSIRT) działające 24/7, w ramach których firma obsługuje m.in. operatorów usług kluczowych.

Thales jest światowym liderem zaawansowanych technologii w trzech obszarach: Obrona i bezpieczeństwo, Lotnictwo i przestrzeń kosmiczna oraz Tożsamość cyfrowa i bezpieczeństwo. Opracowuje produkty i rozwiązania, które pomagają uczynić świat bezpieczniejszym, bardziej ekologicznym i bardziej inkluzywnym. Grupa Thales jest obecna w Polsce od 1992 roku i dostarcza swoim klientom zaawansowane technologicznie rozwiązania dla sektorów, takich jak wojskowość i obronność, tożsamość cyfrowa i cyberbezpieczeństwo oraz lotnictwo i kosmonautyka.

Porozumienie z Ministrem Cyfryzacji obejmuje wszystkie obszary PWCyber: informacyjny, edukacyjny, szkoleniowy i testów oraz certyfikacji.

Firma Trafford IT powstała w 2012r. Od początku swojej działalności specjalizuje się w dostarczaniu starannie wybranych i przetestowanych technologii z zakresu bezpieczeństwa teleinformatycznego, będących światowymi liderami w branży IT i OT. Dostarcza oraz integruje specjalistyczne systemy ochrony przed zaawansowanymi cyberatakami. Skupia się na bezpieczeństwie kluczowych usług klientów, wdrażając między innymi rozwiązania do ochrony baz danych, aplikacji webowych, systemy analizy i wykrywania anomalii czy narzędzi do automatyzowania analizy incydentów w celu zapobiegania cyberatakom. Trafford IT specjalizuje się również w bezpieczeństwie automatyki przemysłowej, co wymaga specjalistycznego i indywidualnego podejścia do realizacji każdego z projektów bezpieczeństwa. W ofercie Trafford IT są także kompleksowe usługi z zakresu SOC, MDR oraz ASO.

Misją Trafford IT jest współtworzyć cyberbezpieczeństwo w Polsce. W tym celu monitoruje trendy i nowe technologie, analizuje zagrożenia i cyberataki. Wszystko po to, aby im zapobiegać lub minimalizować ich skutki. 60-osobowy zespół inżynierów Trafford IT, których ekspercka wiedza jest cyklicznie weryfikowana, potwierdzana branżowymi certyfikatami oraz najwyższymi statusami partnerskimi, gwarantuje najbardziej aktualną i kompleksową wiedzę, unikalne i autorskie metody wdrażania technologii, jakość, terminowość oraz aktywną pomoc w razie wystąpienia incydentów bezpieczeństwa.

Trecom jest polską firmą z ponad 25-letnim doświadczeniem, której głównym obszarem działalności jest projektowanie, wdrażanie i integracja złożonych systemów informatycznych przy jednoczesnym zagwarantowaniu ich bezpiecznego funkcjonowania. Firma wdraża oraz wykorzystuje rozwiązania, które umożliwiają zabezpieczenie każdego obszaru systemów teleinformatycznych, stanowiąc tym samym kompleksowy system cyberochrony dla swoich klientów.

Dzięki stworzonej i świadczonej usłudze Operacyjnego Centrum Bezpieczeństwa (SOC), zespół doświadczonych analityków SOC Trecom przez 24 godziny na dobę zajmuje się zgłoszeniami i monitoruje zdarzenia w systemach w poszukiwaniu znamion incydentów bezpieczeństwa. Jest to możliwe dzięki specjalistycznym narzędziom oraz kompetencjom eksperckim SOC Trecom.

yubico

Firma Yubico została założona w 2007 roku z misją „uczynienia internetu bezpieczniejszym dla wszystkich użytkowników” i jest wynalazcą i producentem klucza YubiKey, który stworzył nowe standardy bezpiecznego logowania w internecie. Klucze sprzętowe YubiKey umożliwiają bezpieczne i łatwe uwierzytelnianie za pomocą różnych protokołów uwierzytelniania (w tym tych odpornych na phishing, takich jak FIDO2 czy SmartCard) bez potrzeby instalowania sterowników lub oprogramowania klienckiego. YubiKey został z powodzeniem wdrożony w wielu firmach (20 z 20 największych spółek technologicznych używa kluczy YubiKey) w ponad 150 krajach.

XOPERO Backup&Recovery

Xopero Software S.A., firma założona w 2009 roku, to pionier w dziedzinie backupu chmurowego w Polsce. Obecnie firma oferuje szeroką gamę produktów dla klientów biznesowych, takich jak Xopero ONE Backup & Recovery (XONE) – oprogramowanie klasy enterprise oraz Xopero Unified Protection (XUP) – wydajne rozwiązanie sprzętowe. Firma jest również właścicielem GitProtect.io - uznawanego za najbardziej zaawansowane rozwiązanie do backupu środowisk DevOps na świecie. Współpracuje z T-Mobile, Orange czy ESET, co umożliwiło jej globalną dystrybucję i ekspansję na rynki zagraniczne. W ramach platformy SphereCyberX 360 firma łączy nowoczesne technologie ochrony danych jak Triple-I w ramach autorskiego podejścia Zero Trust. Produkty Xopero są dostępne na globalnych rynkach, w tym w USA, Australii i Europie Zachodniej. GitProtect.io jest wykorzystywany przez firmy z listy Fortune 500 oraz największe organizacje publiczne.

Rekomendacje Partnerów dotyczące Programu

Z okazji jubileuszu 5-lecia Programu PWCyber, partnerzy zostali poproszeni o rekomendacje w zakresie dalszego rozwoju Programu. Poniżej prezentujemy zintegrowane propozycje, które mają na celu dalszy rozwój i jeszcze bardziej efektywną współpracę pomiędzy rynkiem nowych technologii a administracją.

Pierwsze 5 lat funkcjonowania Programu to intensywne działania w obszarze podnoszenia kompetencji z zakresu cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Rekomendacje partnerów są jednoznacznie zgodne m.in. co do konieczności kontynuacji i rozszerzenia programów szkoleniowych oraz inicjatyw edukacyjnych.

Partnerzy rekomendują utworzenie specjalnego Programu wsparcia dla małych i średnich przedsiębiorstw (MŚP), aby pomóc im w podnoszeniu poziomu zabezpieczeń przed zagrożeniami. Umożliwienie MŚP udziału w pilotażach i testowych wdrożeniach rozwiązań wśród podmiotów krajowego systemu cyberbezpieczeństwa pozwoli na przetestowanie ich produktów w warunkach zbliżonych do rzeczywistych oraz zdobycie cennej informacji zwrotnej. Takie podejście może przyczynić się do zwiększenia innowacyjności i konkurencyjności polskich firm na rynku cyberbezpieczeństwa.

Partnerzy podkreślają również potrzebę tworzenia specjalistycznych grup roboczych, złożonych z przedstawicieli różnych firm i instytucji. Grupy te, pracując nad priorytetowymi zagadnieniami wyznaczonymi przez Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji, umożliwią skuteczne wypracowywanie rekomendacji w formie „white paper", prowadzenie bieżących konsultacji międzysektorowych oraz wymianę wiedzy i doświadczeń. Ponadto, regularne warsztaty i spotkania z ekspertami z różnych branż, takich jak służba zdrowia, energetyka, sektor publiczny czy finansowy, pozwolą na bezpośredni dialog i lepsze zrozumienie specyficznych wyzwań oraz zagrożeń, z jakimi mierzą się poszczególne sektory.

Współpraca w obszarze technologii i innowacji jest niezbędna dla skutecznego przeciwdziałania nowym zagrożeniom. Partnerzy są gotowi wspólnie tworzyć i wdrażać innowacyjne rozwiązania technologiczne, takie jak narzędzia do wykrywania zagrożeń, monitorowania bezpieczeństwa czy ochrony danych z wykorzystaniem sztucznej inteligencji i uczenia maszynowego. Pilotażowe wdrożenia nowych technologii w instytucjach publicznych i podmiotach krajowego systemy cyberbezpieczeństwa umożliwią testowanie i doskonalenie innowacyjnych rozwiązań, co przyczyni się do modernizacji systemów cyberbezpieczeństwa w kraju.

Rozwijanie infrastruktury i narzędzi cyberbezpieczeństwa to kolejny istotny obszar działań. Partnerzy proponują rozwijanie bazy wiedzy, utworzenie helpdesku oraz sekcji pytań i odpowiedzi dotyczących wdrażania nowych regulacji i najlepszych praktyk.

Proponowana jest również współpraca nad rozwojem krajowej platformy chmurowej dla instytucji publicznych i administracji lokalnej, zapewniającej wysoki poziom bezpieczeństwa i odporności na ataki, która przyczyni się do zwiększenia ochrony danych w sektorze publicznym.

Partnerzy zachęcają do organizacji regularnych spotkań networkingowych między partnerami Programu, administracją publiczną i podmiotami krajowego systemy cyberbezpieczeństwa. Tematyczne warsztaty i seminaria skupiające się na aktualnych wyzwaniach i potrzebach uczestników umożliwią wymianę doświadczeń, wiedzy oraz nawiązanie nowych relacji biznesowych. Taka współpraca sprzyja budowaniu sojuszy technologicznych i lepszemu zrozumieniu potrzeb rynku.

Dziękujemy za 5 lat pełnych wyzwań i sukcesów. Przed nami nowy rozdział, który otwiera drzwi do dalszego rozwoju i innowacji. Rekomendacje naszych partnerów są dla nas drogowskazem, który pomoże nam w doskonaleniu realizowanych już przez nas działań, jak i inicjowaniu nowych aktywności, w szczególności u progu wzywań związanych z implementacją do polskiego porządku prawnego Dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii Europejskiej (Dyrektywa NIS2) oraz wdrożenia regulacji mającej na celu certyfikację cyberbezpieczeństwa w Polsce. Dzięki dalszej współpracy w ramach PWCyber będziemy zawsze na bieżąco z najnowszymi rozwiązaniami branży technologicznej oraz wyzwaniami jakie wiążą się z zapewnianiem bezpieczeństwa w tym sektorze gospodarki. Współpraca z branżą IT, w tym ekspertami od rozwiązań bezpieczeństwa, będzie miała wpływ na rozwój odporności kraju na cyberzagrożenia.

Departament Cyberbezpieczeństwa
Ministerstwa Cyfryzacji

Warszawa
2024