CSIRT NASK

PROGRAM PdC

Raport roczny
2024

Spis treści

Słowo wstępne

Szanowni Państwo,

z przyjemnością oddaję w Państwa ręce raport z działalności Programu PdC za rok 2024. Inicjatywa ta odgrywa kluczową rolę jako platforma integrująca wiedzę, doświadczenia i dobre praktyki podmiotów krajowego systemu cyberbezpieczeństwa.

Rok 2024 był okresem intensywnej pracy, ale też licznych inicjatyw: od konsultacji i warsztatów, aż po rozbudowę sieci partnerów Programu PdC. Niezmiernie cieszy mnie rosnące zaangażowanie uczestników, którzy widzą w Programie PdC realne wsparcie i przestrzeń do działania.

W Programie PdC szczególną wagę przywiązujemy do budowania relacji opartych na zaufaniu pomiędzy podmiotami reprezentującymi różne sektory. To właśnie zaufanie stanowi fundament efektywnej współpracy w obszarze cyberbezpieczeństwa.

Dziękuję wszystkim partnerom za kolejny rok współpracy. Przed nami nowe wyzwania, którym stawimy czoła – razem, odpowiedzialnie i z pełnym przekonaniem, że cyberbezpieczeństwo jest naszą wspólną sprawą.

Maciej Siciarek

Dyrektor Pionu CSIRT,
NASK

Podsumowanie Programu PdC - najważniejsze informacje

Rok 2024 był dla Programu PdC czasem dynamicznego rozwoju oraz pogłębiania międzysektorowej współpracy w ramach krajowego systemu cyberbezpieczeństwa.

Program PdC konsekwentnie rozwijał sieć Partnerów oraz umacniał swoją pozycję jako platforma wymiany wiedzy, doświadczeń i dobrych praktyk z obszaru cyberbezpieczeństwa.

Poniżej znajdują się najważniejsze informacje podsumowujące aktywność Programu PdC w 2024 roku – obejmujące główne obszary tematyczne, komunikację oraz rozwój Programu PdC.

Spotkania

12 spotkań

31 prelegentów

46 eksperckich prezentacji

3 szkolenia specjalistyczne

Rozwój

170 Partnerów w Programie PdC

74 nowych Partnerów

+77% wzrost liczby Partnerów w porównaniu do ubiegłego roku

Tematyka

Prawo i regulacje

Techniczne aspekty cyberbezpieczeństwa

Budowanie świadomości

Psychologiczne aspekty cyberbezpieczeństwa

Sztuczna inteligencja

Dezinformacja

Komunikacja

51 wydań newslettera PdC News

600 subskrybentów

O Programie PdC - wizja, misja i cele strategiczne

Wizja

Program PdC konsekwentnie wzmacnia cyfrową odporność Rzeczypospolitej Polskiej poprzez wspieranie rozwoju współpracy międzysektorowej i zdolności podmiotów krajowego systemu cyberbezpieczeństwa – administracji publicznej, sektora prywatnego i środowisk naukowych.

Program PdC dąży do tego, aby podmioty krajowego systemu cyberbezpieczeństwa były nie tylko właściwie chronione pod względem technologicznym, lecz także świadome ryzyk i gotowe do skutecznego reagowania na zagrożenia – w oparciu o aktualną wiedzę, zaufanie i efektywną współpracę międzysektorową.

Misja

Program PdC dąży do stworzenia efektywnej platformy współpracy, w której podmioty krajowego systemu cyberbezpieczeństwa mogą w sposób skoordynowany i systemowy współpracować na rzecz bezpieczeństwa cyfrowego Polski.

Istotą działania Programu PdC jest budowa międzysektorowych relacji opartych na zaufaniu. Poprzez regularne spotkania, Program PdC stwarza warunki sprzyjające wymianie wiedzy eksperckiej, dzieleniu się doświadczeniami i dobrymi praktykami oraz identyfikacji potrzeb z obszaru cyberbezpieczeństwa.

Realizacja tej misji wpisuje się w strategiczne cele państwa w zakresie budowy nowoczesnego, odpornego i zintegrowanego systemu cyberbezpieczeństwa, w którym współpraca i wymiana wiedzy stanowią fundament skutecznego działania.

Cele strategiczne

- Wzmacnianie współpracy międzysektorowej
- Zwiększanie odporności podmiotów krajowego systemu cyberbezpieczeństwa
- Budowanie kompetencji i świadomości w zakresie cyberbezpieczeństwa
- Wspieranie implementacji krajowych i unijnych regulacji
- Rozwój innowacyjnych form współpracy i wymiany wiedzy
- Budowa zaufania i kultury wspólnej odpowiedzialności za cyberbezpieczeństwo

Rola Programu PdC w krajowym systemie cyberbezpieczeństwa

Program PdC to wspólna inicjatywa Ministerstwa Cyfryzacji i NASK-PIB, której celem jest budowa trwałej i efektywnej platformy współpracy w obszarze cyberbezpieczeństwa. Program PdC powstał z myślą o wspieraniu podmiotów krajowego systemu cyberbezpieczeństwa oraz promowaniu idei wielosektorowej kooperacji – będącej jednym z filarów odporności cyfrowej państwa.

Na mocy ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, NASK – Państwowy Instytut Badawczy pełni rolę jednego z trzech zespołów reagowania na incydenty bezpieczeństwa komputerowego na poziomie krajowym (CSIRT NASK), obok CSIRT GOV i CSIRT MON.

W ramach przydzielonych kompetencji CSIRT NASK odpowiada za monitorowanie, analizowanie i reagowanie na incydenty cyberbezpieczeństwa dotyczące podmiotów spoza sektora rządowego i militarnego – w szczególności obejmując swoim zasięgiem jednostki samorządu terytorialnego, operatorów usług kluczowych i podmioty prywatne.

Program PdC wspieraja realizację misji CSIRT NASK.. Jako platforma współpracy i wymiany wiedzy, Program PdC pełni rolę pomostu pomiędzy CSIRT NASK a szerokim gronem interesariuszy – umożliwiając efektywne przekazywanie informacji o zagrożeniach, ostrzeżeń, analiz technicznych, rekomendacji oraz dobrych praktyk.

Dzięki temu Partnerzy Programu PdC mają dostęp do rzetelnych, aktualnych i praktycznych informacji, które wspierają utrzymanie odpowiedniego poziomu cyberbezpieczeństwa.

Program PdC odpowiada również na potrzebę koordynacji działań międzysektorowych oraz budowy zaufania pomiędzy podmiotami o zróżnicowanych profilach i poziomach dojrzałości cyberbezpieczeństwa.

To właśnie zaufanie i współpraca międzysektorowa są uważane za warunek skutecznego funkcjonowania nowoczesnego systemu reagowania na zagrożenia w cyberprzestrzeni.

Obszary działalności Programu PdC

Program PdC odpowiada na współczesne wyzwania w obszarze cyberbezpieczeństwa, które wynikają zarówno z postępu technologicznego, nowych regulacji prawnych czy zjawisk społecznych.

Prawo i regulacje

Program PdC aktywnie wspiera Partnerów w lepszym rozumieniu zmieniającego się otoczenia prawnego, ze szczególnym uwzględnieniem Dyrektywy NIS2 oraz projektu nowelizacji Ustawy o krajowym systemie cyberbezpieczeństwa. Działania obejmują dyskusje o przepisach, konsultacje oraz prezentację praktycznych rekomendacji wdrożeniowych z kraju i innych państw członkowskich Unii Europejskiej.

Techniczne aspekty cyberbezpieczeństwa

Istotnym elementem aktywności Programu PdC jest wymiana wiedzy i doświadczeń na temat technicznych aspektów ochrony systemów i sieci. Partnerzy są informowani o aktualnych zagrożeniach, trwających kampaniach złośliwego oprogramowania, sposobach przeciwdziałania incydentom bezpieczeństwa oraz funkcjach Systemu s46.

Budowanie świadomości

Program PdC koncentruje się także na rozwoju kompetencji w obszarze kształtowania kultury cyberbezpieczeństwa i budowania świadomości w tym obszarze. Działania obejmują promowanie nowoczesnych narzędzi edukacyjnych oraz tworzenie kampanii informacyjnych.

Psychologiczne aspekty cyberbezpieczeństwa

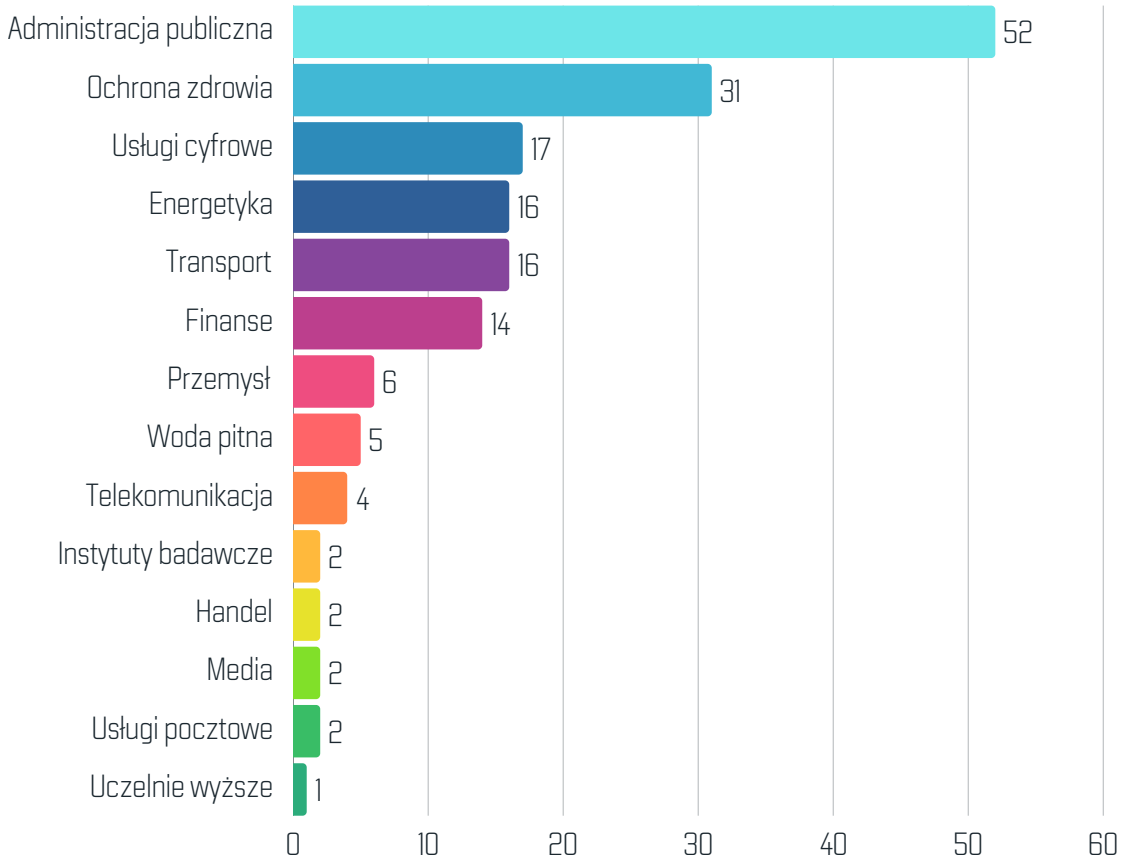
Unikalnym aspektem działań Programu PdC jest propagowanie wiedzy na temat psychologicznych aspektów cyberbezpieczeństwa. Działania obejmują prezentację wyników badań z obszaru cyberpsychologii, omawianie wpływu błędów poznawczych oraz ludzkich podatności na zachowania związane z cyberbezpieczeństwem.

Sztuczna inteligencja i dezinformacja

W odpowiedzi na rosnące znaczenie zagrożeń hybrydowych Program PdC rozszerzył zakres swoich działań o tematykę szkodliwego wykorzystania sztucznej inteligencji – w szczególności deepfake – oraz promowanie strategii przeciwdziałania dezinformacji w środowisku cyfrowym.

Struktura Programu PdC

Program PdC rozwija się dynamicznie, gromadząc wokół wspólnej idei międzysektorowej współpracy coraz szersze grono Partnerów. Zróżnicowana struktura Programu PdC jest jego siłą, ponieważ pozwala na wymianę doświadczeń, wzajemne uczenie się oraz lepsze zrozumienie specyfiki cyberzagrożeń w poszczególnych sektorach. Poniżej przedstawiamy aktualne dane dotyczące liczby partnerów oraz struktury sektorowej Programu PdC.



Najliczniej reprezentowane w Programie PdC są podmioty administracji publicznej oraz ochrony zdrowia.

Istotny udział w Programie PdC mają również podmioty reprezentujące usługi cyfrowe, energetykę, transport i finanse.

170 Partnerów w Programie PdC

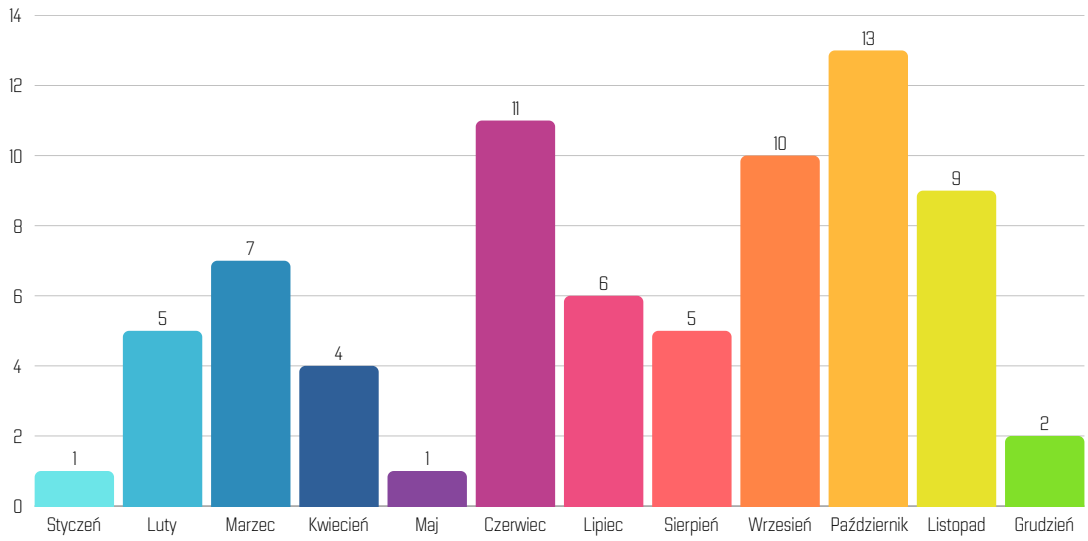
74 nowych Partnerów

+77% wzrost liczby Partnerów

Rozwój sieci Partnerów Programu PdC

Stały rozwój sieci Partnerów stanowi jeden z kluczowych elementów Programu PdC. W 2024 roku odnotowano wyraźny wzrost liczby podmiotów zainteresowanych współpracą, co świadczy o rosnącym znaczeniu wielosektorowej kooperacji w obszarze cyberbezpieczeństwa.

Poniżej przedstawiamy dane dotyczące liczby Partnerów, którzy dołączyli do Programu PdC w roku 2024.



Październik był miesiącem rekordowym, w którym do Programu PdC dołączyła najwyższa liczba nowych Partnerów (13).

W lipcu i sierpniu, mimo sezonu urlopowego, zainteresowanie Programem PdC utrzymywało się na stabilnym poziomie (5) i (6).

Opinie Partnerów o Programie PdC

"Program PdC, w którym Urząd Marszałkowski Województwa Opolskiego uczestniczy od 2017 roku jest bardzo cenną inicjatywą z perspektywy urzędników JST. Zarówno spotkania online, jak i spotkania stacjonarne zawierają mnóstwo praktycznych informacji na temat szeroko rozumianego cyberbezpieczeństwa. Ta wiedza jest szczególnie cenna dla informatyków i urzędników, zwłaszcza tych, którzy pracują w małych gminach i często mają ograniczone możliwości samodoskonalenia."

"W ramach Programu PdC spotykamy się i rozmawiamy o cyberbezpieczeństwie przez cały rok. Spośród wielu wartościowych informacji, które miałam okazję usłyszeć, jeden wniosek szczególnie zapadł mi w pamięć: największym zagrożeniem dla bezpieczeństwa nie jest brak procedur czy przepisów, lecz nasze nieświadome, nieumyślne działania."

"Budowanie świadomości w zakresie security awarness zarówno wśród pracowników jak i w ogóle obywateli, jest kluczową kwestią. Program PdC realizuje to zadania na bardzo wysokim poziomie. My, jako województwo łódzkie, również wspieramy tę inicjatywę i budujemy świadomość wśród mieszkańców i pracowników. Dużym wyzwaniem w kwestii cyberbezpieczeństw jest dla nas szybka wymiana informacji o zagrożeniach. Program PdC pozwala nam na budowę kontaktów z pozostałymi uczestnikami krajowego systemu cyberbezpieczeństwa, co w praktyce przekłada się na poprawę komunikacji."

Zespół Programu PdC

Za realizacją Programu PdC stoi zespół ekspertów NASK, który dba o spójność działań, wysoką jakość merytoryczną i operacyjną efektywność. Na sukces Programu PdC pracuje także wiele zespołów wewnątrz NASK, które ściśle ze sobą współpracują – od specjalistów ds. komunikacji, przez ekspertów merytorycznych, organizatorów wydarzeń oraz zespół technicznego wsparcia. To właśnie synergia kompetencji i efektywna współpraca między zespołami pozwala skutecznie realizować założenia Programu PdC.

Współpraca wewnątrz NASK jest również odzwierciedleniem idei, na której opiera się Program PdC – wspólne działanie, wymiana wiedzy i zaufanie razem budują odporność cyfrową kraju.

Paweł Zegarow

Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni

Paulina Popow

Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni

Dorota Dudzik-Kuleta

Zespół Wsparcia Procesów CSIRT NASK

Marcin Kluczyk

Zespół Wsparcia Procesów CSIRT NASK

Agenda spotkań Programu PdC

Styczeń

Partnerstwo dla Cyberbezpieczeństwa – plany na rok 2024
Paweł Zegarow, Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, NASK

Blockchain, współpraca europejska w ramach EBSI, kolejne wyzwania – cyberbezpieczeństwo technologii przełomowych
Piotr Rutkowski, Zespół Biznesowo-Analityczny Cyberbezpieczeństwa, NASK

Bieżące zagrożenia CERT Polska
Dział Cert Polska, NASK

#Halo! Tu cyberbezpieczny Senior. Społeczna odpowiedzialności biznesu w obszarze budowania świadomości cyberbezpieczeństwa.
Beata Frankiewicz, Zespół Projektów Informacyjno – Popularyzatorskich, NASK

Luty

Cyberbezpieczeństwo infrastruktury krytycznej w świetle dyrektyw CER i NIS2
Monika Stachoń, Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, NASK

Rola CERT Polska w procesie ujawniania błędów w oprogramowaniu
Michał Dondajewski, Dział CERT Polska, NASK

Obowiązki informacyjne podmiotów KSC. Perspektywa NIS2
Grzegorz Mąkosa, Zespół Biznesowo-Analityczny Cyberbezpieczeństwa, NASK

Plan poprawy cyberbezpieczeństwa sektora ochrony zdrowia
Jeremi Olechnowicz, CSIRT CeZ

Agenda spotkań Programu PdC

Marzec

e-IDAS 2. Europejskie portfele cyfrowe

Marcin Idychowski, Zespół Biznesowo-Analityczny Cyberbezpieczeństwa, NASK

Podstawy cyberbezpieczeństwa – budowanie świadomości cyberzagrożeń

Katarzyna Grabowska, Zespół Zarządzania Wiedzą w Obszarze Cyberbezpieczeństwa, NASK

Podnoszenia świadomości w zakresie zagrożeń phishing, ransomware i malware oraz metody rozpoznawania i zapobiegania atakom.

Grzegorz Fiuk, Dział CERT Polska, NASK

Program zarządzania podatnościami w kilku spółkach

Artur Ślubowski, PKP Informatyka Sp. z o. o.

Kwiecień

Wymagania w zakresie bezpieczeństwa – porównanie NIS 2 i AI Act

Emilia Zalewska-Czajczyńska, Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, NASK

Po drugiej stronie incydentu – kto nas atakuje?

Grzegorz Fiuk, Dział CERT Polska, NASK

Budowanie świadomości cyberbezpieczeństwa kluczem do ochrony firmy – opis szkolenia jak budować kampanie i programy świadomościowe

Anna Kwaśnik, Zespół Zarządzania Wiedzą w Obszarze Cyberbezpieczeństwa, NASK

Psychologiczne aspekty cyberbezpieczeństwa – wprowadzenie

Paweł Zegarow, Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, NASK

Agenda spotkań Programu PdC

Maj

Jak zapobiegać wyciekom danych zwiększając świadomość pracowników?
Katarzyna Grabowska, Zespół Zarządzania Wiedzą w Obszarze Cyberbezpieczeństwa, NASK

Psychologiczne aspekty cyberbezpieczeństwa - część 1
Paweł Zegarow, Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, NASK

Krajobraz europejskich ISAC-ów w 2023 r. – prezentacja wyników badania
Paulina Popow, Emilia Zalewska-Czajczyńska, Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, NASK

ISAC – Centra Wymiany i Analizy Informacji w zakresie cyberbezpieczeństwa
Piotr Słowiński, Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, NASK

Panel dyskusyjny - ISAC, jako element krajowego systemu cyberbezpieczeństwa
Piotr Słowiński, Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, NASK

Czerwiec

Ciemna strona AI
Adrian Kapczyński, Wydział Matematyki Stosowanej, Politechnika Śląska

Psychologiczne aspekty cyberbezpieczeństwa - część 2
Paweł Zegarow, Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, NASK

Security Awareness w praktyce
Stanisław Jesiak, AMICA S.A.

Agenda spotkań Programu PdC

Lipiec

Prezentacja poradnika wakacyjnego dla pracodawcy i pracownika
Anna Kwaśnik, Zespół Zarządzania Wiedzą w Obszarze Cyberbezpieczeństwa, NASK

Narzędzia i procesy wspierające podmioty w realizacji zadań wynikających z nowej ustawy o Krajowym Systemie Cyberbezpieczeństwa
Piotr Kudrys, Zespół Rozwoju Systemów Cyberbezpieczeństwa, NASK

Cyber Europe, czyli jak testujemy system cyberbezpieczeństwa
Marcin Napiórkowski, Zespół ds. Szkoleń Specjalistycznych, NASK

Sierpnień

Dane i aktywa informacyjne w kontekście RODO i NIS2
Rafał Prabucki, Uniwersytet Śląski

Psychologiczne aspekty cyberbezpieczeństwa – część 3
Paweł Zegarow, Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, NASK

Prezentacja kompendium edukacyjnego dla JST
Katarzyna Grabowska, Zespół Zarządzania Wiedzą w Obszarze Cyberbezpieczeństwa, NASK

Cyberbezpieczeństwo w Centrum Informatycznych Usług Wspólnych
Bartosz Chumowicz, Centrum Informatycznych Usług Wspólnych Olsztyna

Agenda spotkań Programu PdC

Wrzesień

Cyberzagrożenia – wielkie wyzwanie współczesności
Jarosław Homa, Centrum Cyberbezpieczeństwa, Politechnika Śląska

Nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa
Aleksandra Szczęsna, Dział Prawny

Psychologiczne aspekty cyberbezpieczeństwa – część 4
Paweł Zegarow, Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, NASK

Październik

AI Act – co warto wiedzieć o unijnym rozporządzeniu?
Emilia Zalewska-Czajczyńska, Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, NASK

Dezinformacja: wyzwania w obliczu chaosu informacyjnego
Sylwia Adamczyk, Zespół Zarządzania Wiedzą w Obszarze Cyberbezpieczeństwa, NASK

Bieżące zagrożenia CERT Polska
Krzysztof Chudzik, Dział Cert Polska, NASK

Agenda spotkań Programu PdC

Listopad

Projekt ustawy wdrażającej AI Act
Filip Konopczyński, Biuro Analiz i Badań

Panel dyskusyjny - Zakazane systemy AI
Paweł Zegarow, Monika Stachoń, Piotr Słowiński, Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, NASK oraz Filip Konopczyński, Biuro Analiz i Badań, NASK

Nowelizacja ustawy o krajowym cyberbezpieczeństwa
Krzysztof Michalski, Ministerstwo Cyfryzacji

Podsumowanie efektów pierwszego roku działania ustawy o zwalczaniu nadużyć
Szymon Sidoruk, Dział Cert Polska, NASK

Seminarium narzędziowe – gdzie szukać wzorów i szablonów do organizacji ćwiczeń
Marcin Napiórkowski, Zespół ds. Szkoleń Specjalistycznych, NASK

Zadania operatorów IK i podmiotów krytycznych w znowelizowanej ustawie o zarządzaniu kryzysowym
Witold Skomra, Rządowe Centrum Bezpieczeństwa

Grudzień

Budowanie kultury cyberbezpieczeństwa w oparciu o Dyrektywy CER i NIS II
Dorota Duda, Rządowe Centrum Bezpieczeństwa

Jak skutecznie budować świadomość cyberbezpieczeństwa w organizacji? Szkolenia, materiały, współpraca
Katarzyna Grabowska, Zespół Zarządzania Wiedzą w Obszarze Cyberbezpieczeństwa, NASK

Psychologiczne aspekty cyberbezpieczeństwa
Paweł Zegarow, Zespół Strategii i Rozwoju Bezpieczeństwa Cyberprzestrzeni, NASK

Przyszłość funkcjonowania Systemu S46 w oparciu o projekt ustawy o nowelizacji Krajowego Systemu Cyberbezpieczeństwa
Paweł Chochoł, Zespół Biznesowo-Analityczny Cyberbezpieczeństwa, NASK

Kontakt

Email
pdc@nask.pl

Adres
NASK PIB, Kolska 12, 01-045 Warszawa