NASK

PAŃSTWOWY INSTYTUT BADAWCZY

Cyberbezpieczeństwo
Nauka i biznes

Centrum Badań
i Transferu Technologii

NASK Research Index
Journal N° 1/2019 Rev. 1.7

Słowo od Dyrektora

Drodzy Przyjaciele NASKu,

Cyberbezpieczeństwo staje się obiektem zainteresowania niemal wszystkich instytucji. Potrzebujemy go wszyscy – jako osoby prywatne i jako przedstawiciele przedsiębiorstw, instytucji publicznych czy rządowych. Przez ostatnie 25 lat Państwowy Instytut Badawczy NASK systematycznie budował narzędzia, zespół i kluczowe kompetencje, potrzebne by sprostać ogromnemu wyzwaniu, jakim jest zapewnianie cyberbezpieczeństwa w skali kraju.

Z ogromną przyjemnością pragnę więc przedstawić wiele naukowych projektów oraz gotowych implementacji, które pozwoliły nam opracować mechanizmy detekcji i reakcji na cyberataki, a także rozwijać metody analizy danych i transferu wiedzy. Dziś jesteśmy szczególnie świadomi tego, że cyberbezpieczeństwo musi być wspierane najnowszymi technologiami przetwarzania dużych zbiorów danych oraz metodami sztucznej inteligencji. Wiemy również, że obszar zwany Cyberthreat Intelligence i związane z nim systemy, zbiory danych czy algorytmy wymagają nieustannej aktualizacji, ponieważ wektor potencjalnych zagrożeń zmienia się niezwykle dynamicznie.

Zachęcam do wymiany myśli i doświadczeń – połączmy siły wobec wspólnego wyzwania! Głęboko wierzę, że współpraca interdyscyplinarna i ponadnarodowa jest kluczem do sukcesu w tej dziedzinie.

W niniejszej publikacji przedstawiamy nasze prace i badania nad rozwiązaniami dla cyberbezpieczeństwa, jakie przeprowadziliśmy w Państwowym Instytucie Badawczym NASK.

Inspirującej lektury i do usłyszenia wkrótce!

Dr hab. inż. Jacek Leśkow
Dyrektor NASK

O NAS

CO ZNACZY NASK?

Badania naukowe

Zespół naukowców NASK prowadzi projekty m.in. w obszarze cyberbezpieczeństwa, w których opracowywane są autorskie metody Threat Intelligence wykorzystujące interdyscyplinarny potencjał badaczy

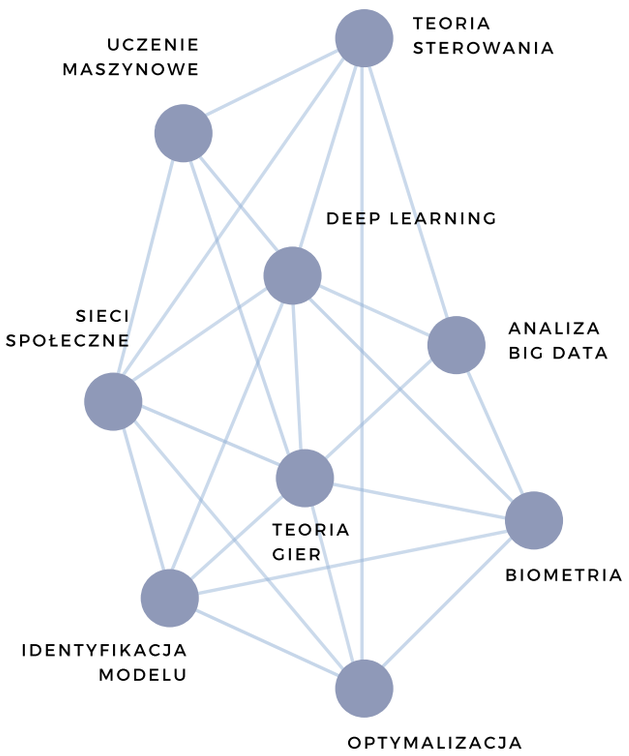
Projekty o randze państwowej

Zgodnie z Ustawą o Krajowym Systemie Cyberbezpieczeństwa NASK sprawuje funkcję zespołu reagowania CSIRT oraz realizuje projekty o znaczeniu strategicznym dla ochrony cyberprzestrzeni RP

Doświadczenie na rynku

NASK posiada własną infrastrukturę telekomunikacyjną oraz szereg produktów i usług z zakresu cyberbezpieczeństwa, które kieruje m.in. do sektora bankowego, szkolnictwa, a także instytucji infrastruktury krytycznej

BADANIA I ROZWÓJ



OBSZARY TEMATYCZNE

Zapewnienie cyberbezpieczeństwa to zadanie niezwykle złożone i wymaga podejścia holistycznego – dlatego nasi badacze sięgają nie tylko po narzędzia tej konkretnej dziedziny, ale odpowiedzi szukają też w dyscyplinach sąsiednich lub wręcz całkiem odległych, a jednak inspirujących.

I tak w realizacji projektów wczesnego wykrywania czy tłumienia cyberataków kluczowe okazały się na przykład badania dotyczące teorii gier, sieci społecznych czy teorii sterowania.

10%

całego zespołu to pracownicy naukowi

25 lat

doświadczenia w IT i cyber-bezpieczeństwie

ponad 700

pracowników zatrudnionych na etatach

100%

wsparcie Ministerstwa Cyfryzacji

DETEKCJA

WCZESNE OSTRZEGANIE

Nauka pozwala patrzeć w przyszłość - nasi badacze dokładają wszelkich starań, żeby być o krok przed atakującym

NASK Cyberbezpieczeństwo

DETEKCJA

ARAKIS Enterprise
NASK

SYSTEM WCZESNEGO OSTRZEGANIA DLA OT/ IT

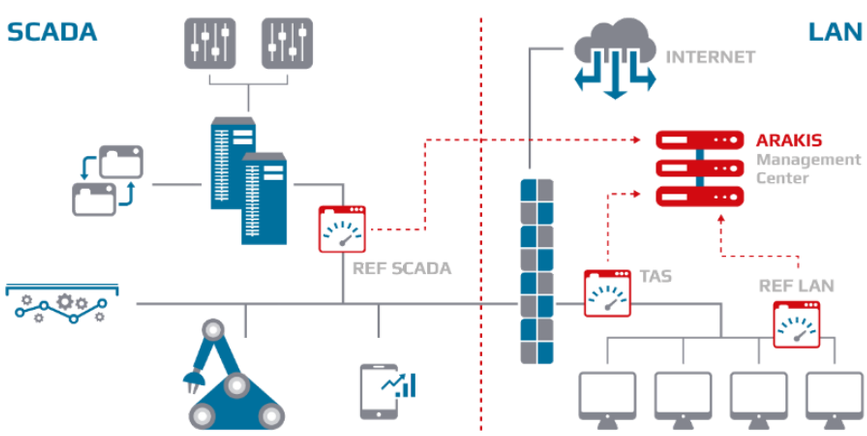
Główną funkcjonalnością systemu jest wykrywanie wzorców zaawansowanych ataków i zagrożeń występujących w sieci, a także generowanie opisu zaobserwowanych incydentów w postaci sygnatur oraz alarmów.

Jednym z podstawowych komponentów systemu ARAKIS 2.0 jest sieć honeypotów, czyli usług pułapek wabiących atakującego oraz rejestrujących jego działania. Skuteczne wykorzystanie ich potencjału wymagało zastosowania w architekturze systemu zaawansowanych metod inżynierii sieciowej redukujących prawdopodobieństwo detekcji obecności pułapki i zwiększających jakość wytwarzanych sygnatur.

INNOWACJA

Efektywne wykrywanie incydentów zagrażających cyberbezpieczeństwu chronionej sieci wymaga sprawnie współdziałających mechanizmów agregacji i korelacji danych rejestrowanych przez sieć sond.
Stworzenie tego systemu to efekt pracy zespołu badawczego nad wieloma odrębnymi zagadnieniami technicznymi i naukowymi, m.in.:

- algorytmami wykrywającymi w czasie wielomianowym podciągi znaków efektywnie charakteryzujące wzorce komunikacji skierowanych do sieci pułapek,
- opartym na uczeniu maszynowym probabilistycznym modelu zapytań kierowanych do serwera oraz opracowanie procesu testowania hipotez oceniających zgodność tych zapytań z wykrytym wzorcem.



DETEKCJA

ARAKIS Enterprise
NASK

SYSTEM WCZESNEGO OSTRZEGANIA DLA OT/ IT

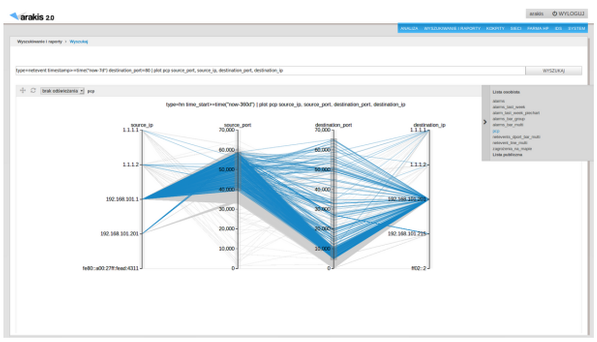
ARCHITEKTURA

System ARAKIS 2.0 zasilany jestdanymi przesyłanymi przez cztery kategorie sensorów:

- reflektor: sensor odpowiedzialny za utrzymywanie komunikacji pomiędzy odpowiednio skonfigurowanymi adresami usług pułapek i farmą honeypotów zbierającą dane na temat rejestrowanych zagrożeń oraz nadużyć w sieci chronionej,
- forwarder: sensor odbierający i przekazujący logi zewnętrznych systemów bezpieczeństwa, m.in.zapór sieciowych (firewalli) oraz systemów antywirusowych,
- TAS: sensor odpowiedzialny za wykrywanie w monitorowanym ruchu niebezpiecznych komunikacji, m.in. z sieciami botów (botnet), oraz przesyłanie informacji o podejrzanych zdarzeniach do centrum systemu ARAKIS 2.0,
- sensor SCADA: sensor odpowiedzialny za utrzymywanie komunikacji z siecią pułapek wyposażonych w emulowane usługi systemów automatyki przemysłowej.

Dzięki modułowej architekturze system ARAKIS 2.0 można łatwo rozbudowywać o kolejne serwisy. Istotnym elementem systemu jest graficzny interfejs użytkownika umożliwiający:

- zarządzanie komponentami systemu,
- analizę i wizualizację danych,
- wyszukiwanie danych przy użyciu autorskiego języka AQL (Arakis Query Language),
- automatyczne generowanie raportów, integrowanych z danymi z klasy SIEM,
- komponowanie paneli operatorskich, dostosowanych do potrzeb użytkownika.



Obecnie intensyfikowane są między innymi prace nad modułami korelacji wykorzystującymi zaawansowane algorytmy sztucznej inteligencji.

DETEKCJA

SISSDEN

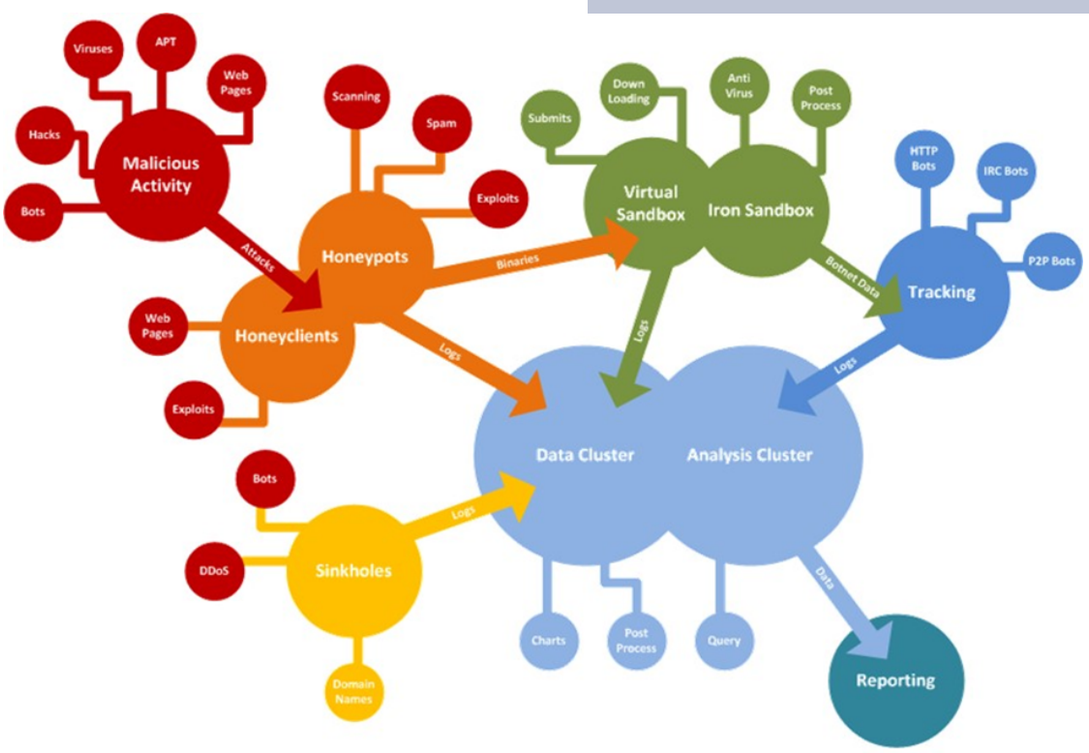
SECURE INFORMATION SHARING SENSOR DELIVERY EVENT NETWORK

Projekt ten jest realizowany przy współpracy z SHADOWSERVER. W jego ramach rozwijane są narzędzia niezbędne do akwizycji, opracowania i analizy ogromnych ilości danych pozyskiwanych z przeróżnych źródeł.

Jądrem projektu SISDEN jest ogólnoświatowa sieć sensorów, którą opracowują i obsługują członkowie konsorcjum. NASK z powodzeniem pełnił rolę koordynatora tak wielkiego międzynarodowego projektu.

Innowacją i sporym wyzwaniem, którego podjęli się badacze, jest zaprojektowanie zarówno architektury tak złożonego, wysoce skalowalnego systemu, jak i opracowanie algorytmów i narzędzi pozwalających na jego sprawne funkcjonowanie.

Baza ta jest absolutnie niezbędna dla powodzenia praktycznego wdrożenia systemów wczesnego wykrywania czy reagowania na cyberataki, zarówno na poziomie publicznym jak i komercyjnym.



THE SHADOWSERVER MODEL

DETEKCJA

SISSDEN

SECURE INFORMATION SHARING SENSOR DELIVERY EVENT NETWORK

Nasi badacze stworzyli innowacyjną architekturę globalnej sieci sensorów (212 sensorów w 53 krajach, co łącznie daje już możliwość monitorowania blisko 900 adresów), która przyczynia się do powstania bazy o największej liczbie precyzyjnie dobranych, najbogatszych w informacje danych potrzebnych do identyfikacji złośliwego oprogramowania i zachowań, opartej na doświadczeniu użytkownika końcowego.

W ramach projektu opracowano szereg nowatorskich rozwiązań:

- metody ciągłego śledzenia konfiguracji botnetów, obejmujące rozszerzenia wcześniejszego systemu do ekstrakcji konfiguracji z zebranych próbek złośliwego oprogramowania
- nowy system emulujący rzeczywiste boty w celu ciągłego śledzenia zmian konfiguracji,
- rozbudowany zestaw metod analizy danych darknetowych umożliwiających bieżącą identyfikację różnych klas obserwowanych zjawisk
- metodę analizy dialektów SMTP umożliwiającą identyfikację rodzaju oprogramowania klienckiego i serwerowego używanego przy przesyłaniu poczty elektronicznej na podstawie drobnych różnic w implementacji protokołu. Metodę tę można wykorzystywać do niezależnej od treści identyfikacji spamu oraz identyfikacji botnetów odpowiedzialnych za poszczególne kampanie spamowe.

INNOWACJA

autorski algorytm wykrywający algorytmy generacji pakietów (PGA) wyłącznie na odstawie obserwacji ruchu sieciowego, ale w przeciwieństwie do typowych systemów tutaj zastosowano zaawansowany algorytm,który wykrywa wiele typów zależności między poszczególnymi polami nagłówków pakietów w ramach grupy i dopiero konstruuje regułę.

REAKCJA

WYKRYWANIE I REAGOWANIE

Mimo zaawansowanych mechanizmów ostrzegania, incydenty zagrażające cyberbezpieczeństwu wciąż jeszcze się zdarzają. Dlatego liczą się: szybkie wykrywanie i skuteczna reakcja.

NASK Cyberbezpieczeństwo

REAKCJA

SYSTEM DETEKCJI I MITYGACJI ANTY-DDOS

FLDX to najnowszej generacji system wykrywania i tłumienia ataków wolumetrycznych typu DDoS.

System może działać w trybie w pełni automatycznym, półautomatycznym lub jako wspomaganie decyzji dla operatora ludzkiego – w zależności od potrzeb i założeń klienta. Na efektywność systemów typu anty-DDoS składają się nie tylko skuteczność działania, ale również czas reakcji.

W systemie FLDX autorskie podejście do detekcji, uzyskane dzięki naukowemu sformułowaniu problemu, pozwoliło osiągnąć wyjątkowy wynik - **czas mijający od wykrycia do pełnego stłumienia wynosi średnio 10 sekund.**

INNOWACJA

To system, który dzięki niestandardowej metodzie detekcji wykrywa nie tylko znane ataki, ale w lot dostosowuje się do zmieniającego się wektora cyberzagrożeń odpowiadając na nowe, nieznane dotąd wzorce ataków.

Co więcej, zastosowana technologia, oparta na modelu matematycznym opracowanym przez zespół badaczy NASK, sprawia, że **wykryty atak tłumiony jest w sposób możliwie nieinwazyjny dla reszty sieci.** FLDX niczym najwprawniejszy selekcjoner oddziela połączenia zainfekowane od tych zdrowych, co pozwala skutecznie mitygować ataki jednocześnie nie blokując dostępu do innych usług.

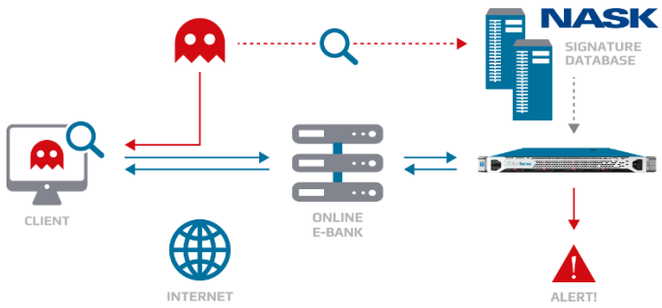
REAKCJA

BotSense
NASK

SYSTEM MONITOROWANIA BANKOWOŚCI INTERNETOWEJ

System BotSense jest skierowany do sektora finansowego, gdzie odpowiada za wykrywanie w czasie rzeczywistym prób przejęcia kont i nieautoryzowanych transakcji, na które użytkownicy narażeni są podczas korzystania z bankowości elektronicznej.

Za system umożliwiający klientom banku bez obaw korzystanie z internetowych rozwiązań, NASK otrzymał nagrodę „Portfel WPROST 2017" w kategorii bezpieczeństwo.



7 mln

kont e-bankowości skutecznie monitorowanych przez BotSense

IDEA

Sukces systemu polega na dobrze opracowanym i zrealizowanym pomyśle na jego architekturę (kod JavaScript umieszczany w kodzie serwisu transakcyjnego banku, oparty na metodach m.in. analizy behawioralnej i fingerprintingu), oraz na dostępie NASK do bogatej i wciąż aktualizowanej bazy własnych i partnerskich kanałów informacji o sygnaturach złośliwego oprogramowania, dzięki czemu bank może w czasie rzeczywistym identyfikować zagrożenia.

Ogromną zaletą systemu Botsense jest zachowanie zasady prywatności, ponieważ **gwarantuje pełną funkcjonalność bez konieczności pobierania danych wrażliwych** o klientach banku.

REAKCJA

RegSOC

REGIONALNE CENTRUM CYBERBEZPIECZEŃSTWA

Celem projektu RegSOC jest przygotowanie i **praktyczne wdrożenie prototypu modelowego Regionalnego Centrum Bezpieczeństwa Cyberprzestrzeni (RegSOC) dla podmiotów publicznych, w oparciu o wyniki badań naukowych.**
W ramach projektu przeanalizowana zostanie zdolność do rozszerzenia współpracy na sektor prywatny.
Współpracując z Krajowym Centrum Bezpieczeństwa Cyber-przestrzeni, Centrum może stanowić element wielopoziomowego systemu bezpieczeństwa cybernetycznego Polski.
Projekt ma na celu podniesienie poziomu ochrony bezpieczeństwa, wprowa-dzenie procedury zmniejszania prawdopodobieństwa wystąpienia niepożądanych zdarzeń oraz surowe metody obniżania ich skutków.
Projekt będzie realizowany przez Konsorcjum następujących instytucji: Akademia Górniczo-Hutnicza we Wrocławiu (WCSS) - Lider, Państwowy Instytut Badawczy NASK, Instytut Innowacyjnych Technologii EMAG.

Projekt ten jest współfinansowany przez Narodowe Centrum Badań i Rozwoju w ramach programu CyberSecIdent Cyberbezpieczeństwo oraz e-Tożsamość.

Oczekiwane rezultaty projektu:

- stworzenie urządzenia wraz z oprogramowaniem dla podmiotów publicznych, zdolnego do pracy jako urządzenie autonomiczne w ramach administracji lokalnej, a także zintegrowane z RegSOC;
- stworzenie platformy monitoringu bezpieczeństwa cybernetycznego na potrzeby RegSOC. Na platformę składać się będzie oprogramowanie oraz architektura organizacyjna (modele zarządzania i procedury organizacyjne);
- opracowanie procesowego i organizacyjnego modelu działania centrów regionalnych we współpracy z NCCyber, wraz z wewnętrznym oprogramowaniem integrującym RegSOC z Krajową Platformą Bezpieczeństwa Cyberprzestrzeni (NPC);
- wdrożenie modelu RegSOC, z komponentami klienckimi zaimplementowanymi w wybranych naukowych podmiotach zainteresowanych wynikami projektu;

ANALIZA

ANALIZA BIG DATA

W cyberbezpieczeństwie
najważniejszą walutą jest informacja,
dlatego z powodzeniem rozwijamy narzędzia
do pozyskiwania, analizy i obróbki danych.

NASK Cyberbezpieczeństwo

ANALIZA

Forensic Lab

ZAAWANSOWANE LABORATORIUM KRYMINALISTYKI CYFROWEJ

Stworzone w ramach projektu metodyki i procedury działania laboratorium pozwolą na zwiększenie wykrywania cyberprzestępstw oraz eliminowanie działań szkodliwych, w szczególności tych związanych ze zorganizowanymi grupami przestępczymi. Tworzenie laboratoriów kryminalistyki śledczej jest kolejnym etapem rozwoju zespołów reagowania na ataki w sieciach (typu CERT), a także stanowi naturalną konieczność dla organów ścigania. Tworzenie tego typu laboratoriów w pełni odpowiada światowym trendom.

Wnioski z działań laboratorium mogą wprost doprowadzić do stworzenia nowych bezpiecznych produktów lub usług teleinformatycznych w cyberprzestrzeni dzięki detekcji i eksploracji aktualnych słabych punktów i zagrożeń.

Projekt pozwala przeanalizować techniki lepszego badania ataków i ich skutków. Dzięki opracowanym rozwiązaniom podmioty wykorzystujące metody analizy powłamaniowej uzyskają przewagę nad podmiotami, które nie posiadają tej wiedzy, poprzez potencjalnie szybką implementację nowych zabezpieczeń. A w efekcie podmioty te uzyskają przewagę konkurencyjną dzięki zwiększonej odporności na rozpoznane ataki.

laboratorium kryminalistyki cyfrowej

Politechnika Warszawska

Projekt umożliwia bezpośrednią współpracę pomiędzy Politechniką Warszawską a NASK, a wtórnie z organami ścigania, które wymagają precyzyjnych i szybkich metod zbierania i analizy dowodów cyfrowych.

CELE

Cele projektu:

- wypracowanie metodyk i procedur zbierania i analizy cyfrowych dowodów;
- zbudowanie wzorcowego laboratorium, z modułem mobilnym;
- rozwój metod ochrony przed nowymi atakami np. typu ransomware.

ANALIZA

NPC NARODOWA PLATFORMA CYBERBEZPIECZEŃSTWA

NARODOWA PLATFORMA CYBERBEZPIECZEŃSTWA

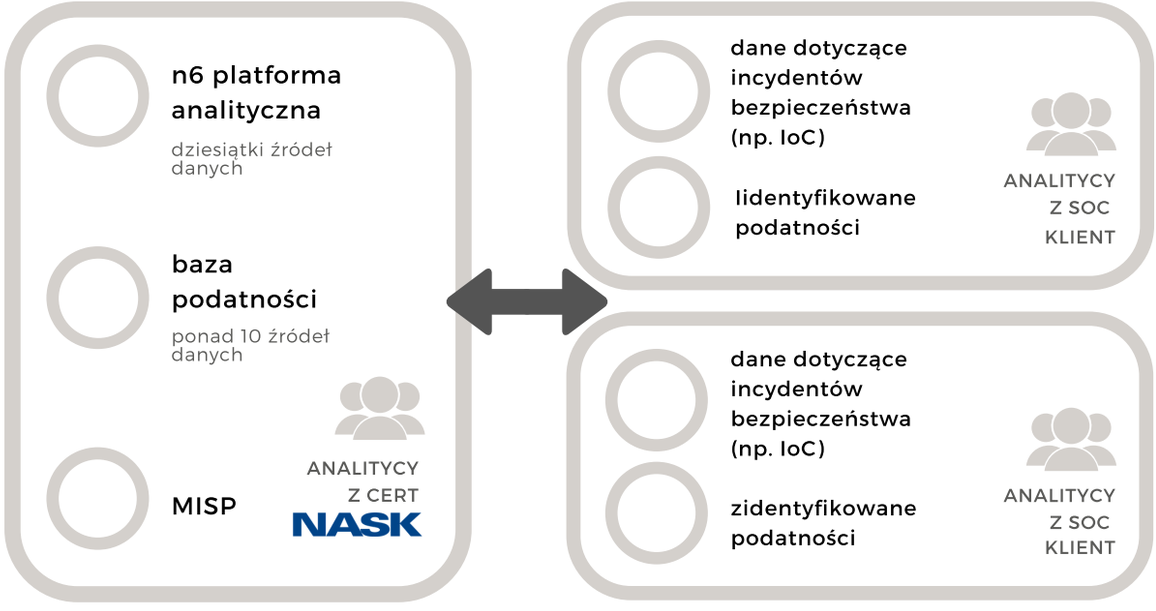
Celem projektu jest opracowanie eksperckiego systemu wspierającego wybór odpowiednich metodyk i miar wyznaczających wymogi bezpieczeństwa teleinformatycznego oraz raportowania istotnych incydentów naruszających bezpieczeństwo teleinformatyczne dla poszczególnych sektorów objętych Dyrektywą NIS oraz Ustawą o Krajowym Systemie Cyberbezpieczeństwa. Rezultatem końcowym projektu będzie podniesienie poziomu cyberbezpieczeństwa Rzeczypospolitej Polskiej oraz zwiększenia potencjału narodowego i kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni.

INNOWACJA

NPC oferuje nowatorskie metody i narzędzia skoncentrowane na:

- korelacji zdarzeń, analizy sytuacyjnej, dynamicznej i statycznej analizy ryzyka;
- metodach i technikach wielowymiarowej wizualizacji z wielomodalnym interfejsem operatora;
- wykrywaniu podatności oraz zagrożeń występujących w sieciach TCP/IP, mobilnych sieciach bezprzewodowych, środowisku IoT, sieciach automatyki przemysłowej oraz
- bezpiecznych mechanizmach udostępniania informacji pomiędzy Centrum Operacyjnym a użytkownikami Platformy.

KONCEPCJA TRANSFERU WIEDZY I CROWDSOURCINGU



ANALIZA

NARODOWA PLATFORMA CYBERBEZPIECZEŃSTWA

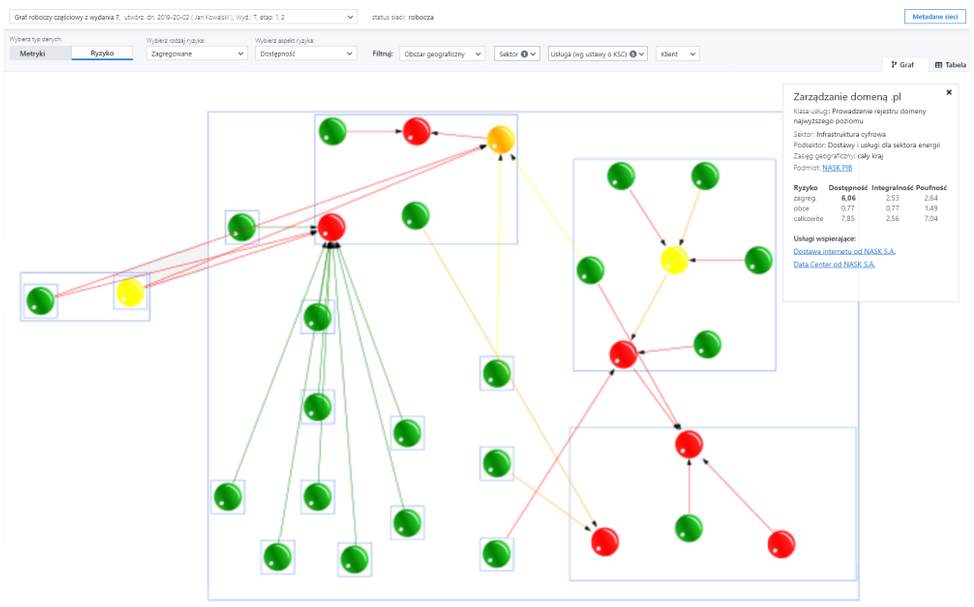
Istotny moduł platformy stanowi wspomaganie decyzji i analiza ryzyka.

Moduł ekspercki służy do wydawania automatycznych rekomendacji na podstawie przeprowadzonej przez system centrum operacyjnego NPC analizy ryzyka. Automatyzacja ta ma za zadanie odciążyć analityków oraz skrócić czas przepływu informacji na temat przekroczenia wartości progowej przez jedną lub więcej zgłoszonych usług, lub o wzroście zagrożenia w całym sektorze, w którym prowadzona jest działalność gospodarcza.

INNOWACJA

Metoda hierarchizacji umożliwia zdefiniowanie krytyczności powiązań elementów infrastruktury teleinformatycznej z usługami wspierającymi wewnętrznymi za pomocą macierzy, bo opisuje jaki wpływ na poufność, integralność i dostępność usługi wspierającej wewnętrznej miałoby zakłócenie lub zupełna kompromitacja poszczególnych aspektów danego elementu infrastruktury ICT.

Elementem wizualizacji takiej struktury hierarchicznej są grafy. Najpierw tworzona jest macierz incydencji pomiędzy poszczególnymi usługami, następnie stosowane są algorytmy kolorowania grafu, które pozwalają zilustrować stopień krytyczności jednych usług względem pozostałych.



ANALIZA

BioMobi

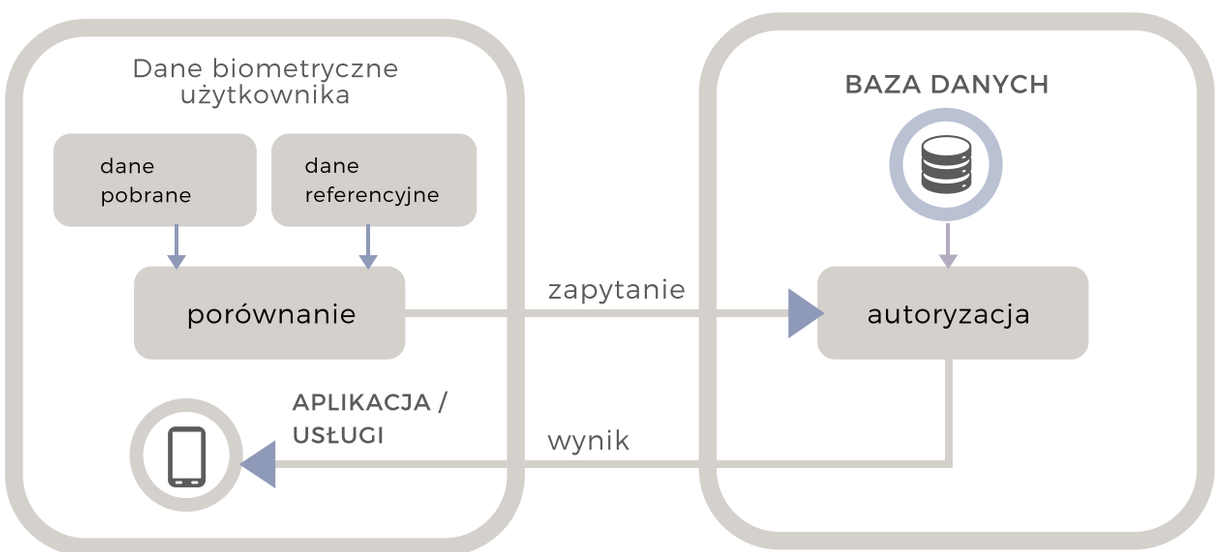
MOBILNY SYSTEM ZDALNEJ AUTORYZACJI NA NIEWYSPECJALIZOWANE URZĄDZENIA MOBILNE

Celem projektu jest zbudowanie mobilnego systemu zdalnej, mutli-modalnej, adaptacyjnej, biometrycznej autoryzacji z wykorzystaniem gotowych urządzeń mobilnych.
Nasze rozwiązanie integrujemy z istniejącymi na rynku urządzeniami, dzięki czemu uwierzytelnianie biometryczne staje się łatwiej i szerzej dostępne. Adaptacyjność systemu polega na dostosowaniu poziomu bezpieczeństwa uwierzytelniania biometrycznego do wymagań strony autoryzującej (bank, szpital, urząd państwowy, uczelnie itp.).

Przez multimodalność rozumiemy zastosowanie szerokiej klasy modalności biometrycznych, takich jak twarz, głos, odcisk palca, dłoń, konieczne jest przyjęcie wyższych standardów bezpieczeństwa w zakresie transmisji i przechowywania danych.

INNOWACJNE WYNIKI

- niezależny system oparty na powszechnie dostępnych urządzeniach mobilnych, zapewniający łatwy dostęp do biometrycznego uwierzytelniania;
- autorskie algorytmy biometryczne dla różnego rodzaju modalności biometrycznych wykorzystujące metody sztucznej inteligencji, takie jak konwolucyjne sieci neuronowe
- zastosowanie autorskich algorytmów zwiększa odporność na ataki prezentacyjne, przez co akwizycja danych w środowiskach niekontrolowanych staje się bezpieczniejsza
- możliwość dostosowania systemu poprzez wykorzystanie wybranych modalności przy jednoczesnym zachowaniu wymogów bezpieczeństwa;
- nowe metody bezpiecznego pozyskiwania i przechowywania danych biometrycznych;



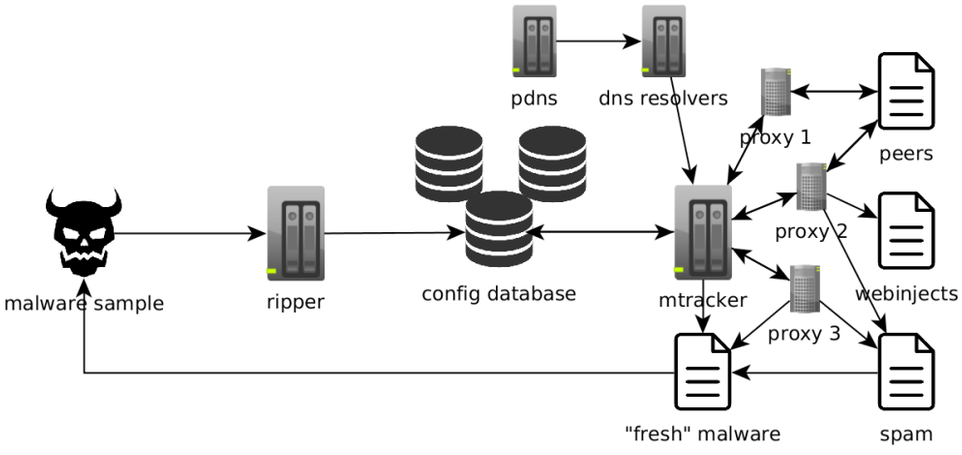
mTracker

NARZĘDZIE DO ZAAWANSOWANEJ AKWIZYCJI I ANALIZY DANYCH

W walce z botnetami istotne jest nie tylko szybkie i skuteczne unieszkodliwienie aktualnego ataku, ale też pobranie próbki danych i ich głęboka analiza. Poznanie mechanizmów działania stojących za tego typu atakami może pozwolić na jeszcze skuteczniejszą reakcję, a także jeszcze efektywniejsze ich wykrycie, jeszcze zanim zdążą się w pełni uaktywnić. Pozyskane na próbkach malware'u informacje pozwalają też na symulowanie działania rzeczywistych botnetów i samodzielne komunikowanie się z serwerami C&C.

Opracowany przez zespół CERT mTracker to narzędzie do pozyskiwania i analizy jak największej ilości danych z wielu botnetów. Dzięki czemu udaje się odtworzyć m.in. injecty, szablony spamu czy próbki innych rodzin złośliwego oprogramowania.

Jako że używanie domen w TLD ,.bit' (dostarczanych przez Namecoin) jest coraz popularniejsze w złośliwym oprogramowaniu, musieliśmy dostarczyć nasz własny resolver (domeny ,.bit' nie są oficjalnie dostępne przez główne serwery DNS). Po implementacji tej funkcji zauważyliśmy kolejną szansę – często domeny C&C są zdejmowane szybko po rozpoczęciu kampanii (przez organy ścigania albo zespoły CERT), ale serwer ciągle odpowiada pod swoim oryginalnym adresem IP. Z tego powodu, gdy rozwiązywanie nazwy domeny się nie powiedzie (albo zostanie rozwiązana do sinkholowanej domeny) używany danych z innego naszego systemu – pasywnego DNS:



ANALIZA

NECOMA

NIPPON-EUROPEAN CYBERDEFENSE-ORIENTED MULTILAYER THREAT ANALYSIS

Projekt powstawał w ramach współpracy europejsko-japońskich konsorcjów naukowo-komercyjnych. Badacze z NASK PIB pracowali tu przede wszystkim nad rozwijaniem narzędzi do agregacji dużej ilości danych oraz zaawansowanych mechanizmów inferencyjnych wykorzystanych do analizy zagrożeń.
Zbiór danych wykorzystywanych do uczenia klasyfikatorów i mechanizmów opartych na regułach musi być z jednej strony liczny, z drugiej za odpowiednio zawężony, by pozwalać na maksymalnie skuteczne wykrywanie zagrożeń przy jak najmniejszym błędzie (fałszywych alarmach), dlatego w ramach projektu NECOMA opracowywana była metodyka oceny źródeł, z których pochodzą informacje, pod kątem ich jakości.

Jednym z kluczowych dla projektu narzędzi stanowiących źródło danych o złośliwym oprogramowaniu była stworzona przez CERT Polska platforma n6 (autorska baza malware'u), dlatego w ramach projektu prowadzono również prace nad jej udoskonaleniem (dodanie możliwości strumieniowego przekazywania zdarzeń w celu zminimalizowania opóźnień w komunikacji) oraz opublikowano n6 SDK na otwartej licencji GPL.

総務省
Ministry of Internal Affairs and Communications

SEVENTH FRAMEWORK PROGRAMME

INNOWACJA

W projekcie wykorzystano między innymi algorytm FP-Growth (Frequent Pattern) – adresy URL są parsowane i kompresowane do postaci drzewa FP, które z kolei poddawane jest eksploracji przy użyciu strategii „dziel i rządź” („divide-and-conquer strategy”) opracowanej przez Y. Han (2000). Implementacja tej metody odkrywania wiedzy posłużyła do stworzenia zestawu uczącego dla klasyfikatora maszyny wektorów nośnych, którego zadaniem jest przypisywanie nowych podejrzanych wzorców do kategorii „powiązany” lub „nie powiązany” z kampanią złośliwą. Adaptacja zaawansowanych metod z zakresu data mining miała istotne znaczenie dla poprawy jakości ostrzegania o zagrożeniach.

TRANSFER

TRANSFER WIEDZY I TECHNOLOGII

Zbierając i opracowując dane
wytwarzamy wiedzę i technologie,
którymi chcemy się dzielić,
by zwiększać bezpieczeństwo.
Wspólnie możemy więcej!

NASK Cyberbezpieczeństwo

WIEDZA

Cybersecurity Certification

KRAJOWY PROGRAM CERTYFIKACJI BEZPIECZEŃSTWA ORAZ PRYWATNOŚCI PRODUKTÓW I SYSTEMÓW IT ZGODNY Z COMMON CRITERIA

Celem projektu KSO3C jest stworzenie programu ewaluacji i certyfikacji cyberbezpieczeństwa teleinformatyki. Projekt realizowany jest w ramach współpracy trzech jednostek naukowo-badawczych, tj. Instytutu Łączności, NASK PIB oraz Instytutu Technik Innowacyjnych EMAG, znajdujących się pod bezpośrednim nadzorem Ministerstwa Cyfryzacji. Projekt ma na celu stworzenie i implementację narodowego programu certyfikacji bezpieczeństwa i prywatności tele-informatyki w oparciu o normę Common Criteria (CC). Realizacja tego zadania jest odpowiedzią na inicjatywę Komisji Europejskiej dotyczącą stworzenia europejskich ram certyfikacji cyber-bezpieczeństwa produktów i usług IT.

Końcowym rezultatem projektu będzie **w pełni funkcjonujący program certyfikacji, w ramach którego będą wydawane certyfikaty o między-narodowej rozpoznawalności.** Program certyfikacji będzie posiadał strukturę otwartą na inne podmioty, które chciałby do niego przystąpić jako laboratoria przeprowadzające ewaluację produktów bądź usług.
Warunkiem przystąpienia do współpracy jest spełnianie europejskich standardów dotyczących oceny zgodności, w tym bezstronności i transparentności.

NOWE METODY

Certyfikacja i ewaluacje urządzeń elektronicznych wymagają najbardziej zaawansowanych metod testowania ich potencjalnych podatności. W związku z tym jednym z celów projektu jest opracowanie nowych metod do oceny bezpieczeństwa i poufności danych użytkowników. W celu zapewnienia wysokiego poziomu zaufania do produktów, będą one sprawdzane przy zastosowaniu technik zarówno inwazyjnych, jak nieinwazyjnych, w tym:

- inżynieria odwrotna
- rozszerzenie metod analizy podatności (AVA_VAN)
- ataki typu side-channel
- precyzyjne metody ataków chipów kryptograficznych, takie jak iniekcje laserowe (fault injection)

PROJEKT KSO3C (CYBERSECIDENT/381282/I/NCBR/2017) JEST FINANSOWANY PRZEZ NARODOWE CENTRUM BADAŃ I ROZWOJU W RAMACH PROGRAMU CYBERSECIDENT

DANE

Cybersecurity Certification

POLISH SCHEME FOR SECURITY AND PRIVACY **EVALUATION AND CERTIFICATION** OF IT PRODUCTS AND SYSTEMS COMPLIANT WITH **COMMON CRITERIA**

Standard CC definiuje tzw. profile zabezpieczeń (Protection Profiles – PP), które formułują metody zabezpieczeń danej klasy produktów. Profile te podlegają ocenie (walidacji) przez kompetentny personel pod kątem ich kompletności i efektywności proponowanych w nich metod zabezpieczeń produktu. Pomaga to potencjalnym kupującym poprawnie formułować wymagania względem bezpieczeństwa produktu, jak również producentom w tworzeniu bardziej bezpiecznych produktów. W tym drugim przypadku deweloper może opracować tzw. zadanie zabezpieczeń (Security Target – ST) dla swojego produktu. Na jego podstawie przeprowadzona zostanie ocena bezpieczeństwa produktu przez zaufaną trzecią stronę, która zweryfikuje, czy wymagania względem cyberbezpieczeństwa są spełnione, zastosowane rozwiązania są skuteczne i czy produkt nie posiada żadnych znanych podatności.

ZNACZENIE

Poza wymaganiami standardu Common Criteria, wszystkie strony projektu mają na celu uzyskanie akredytacji względem norm ISO/IEC 17025 oraz 17065. Ma to na celu potwierdzenie spełnienia najwyższych standardów w zakresie bezstronności i poufności.

Celem projektu KSO3C jest stworzenie programu będącego kwalifikowanym członkiem dwóch międzynarodowych porozumień o wzajemnej rozpoznawalności – SOG-IS MRA i CCRA. Zapewni to możliwość wydawania certyfikatów honorowanych w 30 krajach na całym świecie

TECHNOLOGIE

n6

AUTORSKA BAZA SŁUŻĄCA DO GROMADZENIA, PRZETWARZANIA I PRZEKAZYWANIA INFORMACJI O INCYDENTACH W SPOSÓB AUTOMATYCZNY

Otwarty system stworzony z myślą o gromadzeniu, przetwarzaniu i przekazywaniu informacji o zdarzeniach bezpieczeństwa w sieci. Platforma n6 w pełni automatycznie pobiera dziesiątki milionów informacji na temat incydentów z Polski i świata. Dane dostarczane są wieloma kanałami, m.in. wykrywane w wyniku systemów wykorzystywanych przez podmioty zewnętrzne oraz wewnętrznych systemów obsługiwanych przez zespoły NASK. Dodatkowym źródłem informacji o sieciach klienta mogą być wyniki działań operacyjnych CERT Polska.

Rozbudowany system tagowania katalogowanych incydentów pozwala przypisywać je do konkretnych podmiotów, dzięki czemu agregacja danych jest uporządkowana, a specjalnie przygotowana paczka zawiera oryginalny format źródła. Informacje o źródłach ataku przekazywane są w postaci URLi, domen, adresów IP lub nazw malware'u.

Projekt ma charakter otwarty i będąc właścicielem, operatorem lub administratorem sieci można zgłosić chęć dostępu do danych zawierających się w platformie.

SOASP

ROZSZERZENIE FUNKCJI CUCKOO SANDBOX

W ramach projektu SOASP opracowaliśmy rozszerzenia funkcji Cuckoo Sandxbox, czyli systemu zautomatyzowanej analizy złośliwego oprogramowania.
Rozszerzenia te obejmują techniki wspomagające analizę statyczną próbek malware'u, z naciskiem na przetwarzanie rozpakowanych plików binarnych oraz zdobywanie konfiguracji statycznej. Tworzone przez nasz zespoł moduły do deszyfracji komunikacji oraz stosowania reguł Yara w odpowiednio zdefiniowanych sytuacjach są **publikowane w trybie open source**.

Portal „No more ransom”

PORTAL OFERUJĄCY POMOC OFIAROM CYBERATAKÓW

W związku z narastającą skalą ataków typu ransomware, w trzecim kwartale 2016 roku powstał serwis No More Ransom, który za cel postawił sobie walkę z tym zagrożeniem oraz pomoc ofiarom ataków. Inicjatorami byli Europol, National High Tech Crime Unit (holenderska jednostka policji do zaawansowanej technologicznie przestępczości), Kaspersky Lab oraz McAfee.

Podejmowane w ramach projektu działania mają głównie charakter edukacyjny i wskazują użytkownikom, jak uniknąć infekcji. Serwis służy również do dystrybucji dekryptorów do niektórych rodzin ransomware.

CENNA POMOC

CERT dołączając do projektu udostępnił własne dekryptory do rodzin CryptoMix oraz CryptoShield, a także Mole, należący do tej samej rodziny co CryptoMix, ale korzystający z innego algorytmu szyfrowania. Dektryptory te zostały pobrane niemal 6000 razy z prawie 3000 adresów IP. W przypadku obu odmian ransomware kwoty okupu potrafiły sięgać kilkudziesięciu tysięcy dolarów.

Program EUNITY

Projekt EUNITY promuje dialog w zakresie bezpieczeństwa teleinformatycznego oraz ochrony prywatności pomiędzy Unią Europejską a Japonią i polega na:

- wspomaganiu nawiązywania kontaktów i wymiany doświadczeń,
- określeniu bieżących trendów i wyzwań w obu regionach oraz porównaniu kierunków działań administracji, przemysłu oraz środowisk akademickich,
- zidentyfikowaniu obszarów, w których wskazana jest współpraca europejskich i japońskich firm oraz instytucji,
- porównaniu planów badawczych, legislacji oraz długofalowej polityki w dziedzinie bezpieczeństwa teleinformatycznego,
- wskazaniu potencjalnych mechanizmów finansowania przyszłych europejsko-japońskich projektów badawczo-rozwojowych,
- oraz promocji innowacyjnych rozwiązań stworzonych w Europie i działań, jakie UE podejmuje w obszarze bezpieczeństwa.

ZESPÓŁ REDAKCYJNY

redaktor naczelny
Prof. Ewa Niewiadomska-Szynkiewicz

opracowanie, koncepcja i projekt wydania
dr Inez Okulska

redakcja tekstów
dr Inez Okulska
mgr inż. Paweł K. Kostkiewicz

autorzy
dr inż. Michał Karpowicz
dr inż. Michał Marks
mgr inż. Paweł K. Kostkiewicz
mgr inż. Przemysław Puławski

korekta
mgr inż. Przemysław Puławski

NASK Państwowy Instytut Badawczy
ul. Kolska 12, Warszawa
+48 22 380 82 00
www.nask.pl

NPC NARODOWA PLATFORMA CYBERBEZPIECZEŃSTWA

Narodowe Centrum Badań i Rozwoju

RegSOC

KSO3C

KSO3C, NPC, BioMobi, RegSoc, Forensic Lab to projekty finansowane przez Narodowe Centrum Badań i Rozwoju w ramach programu CyberSecIdent

Badania i rozwój

Państwowy Instytut Badawczy NASK wychodzi naprzeciw wyzwaniom, jakimi są tworzenie innowacyjnych rozwiązań i transfer technologii. Naszą misją jest rozwój współpracy nauki z biznesem.

Jako jednostka badawcza jednocześnie działająca na rynku komercyjnym mamy szczególną pozycję, którą naukowcy i inżynierowie NASK wykorzystują do tego, aby rozwijać nowe technologie i rozwiązania w obszarze ICT, cyberbezpieczeństwa, biometrii oraz sztucznej inteligencji. Efekty pracy naszych badaczy zostały z powodzeniem wdrożone w postaci finalnych produktów lub prototypów, między innymi w instytucjach administracji publicznej, infrastruktury krytycznej oraz u partnerów biznesowych.

Kluczowym obszarem aktywności NASK są działania związane z zapewnieniem bezpieczeństwa Internetu. W strukturze Instytutu funkcjonuje jeden z trzech zespołów reagowania CSIRT (Computer Security Incident Response Team), którego zakres obowiązków określa ustawa o Krajowym Systemie Cyberbezpieczeństwa. CSIRT NASK zajmuje się reakcją na zdarzenia naruszające bezpieczeństwo sieci w Polsce oraz koordynacją działań w tym zakresie.

NASK jest również zaangażowany w działalność edukacyjną i szkoleniową w obszarze cyberbezpieczeństwa i bezpiecznego korzystania z nowych technologii teleinformatycznych.

Prof. Ewa Niewiadomska-Szynkiewicz
Dyrektor Naukowy

NASK

Tym, co odróżnia Instytut Badawczy NASK od ściśle komercyjnych przedsiębiorstw jest podejście do tworzenia rozwiązań dla obecnych i przyszłych potrzeb klientów. Nasi badacze komercyjny problem ujmują w ramy nauki, by za pomocą jej narzędzi, nierzadko szerszych i bardziej abstrakcyjnych, dojść do wyników nie tylko satysfakcjonujących, lecz także innowacyjnych.

Główny nurt badań wyznacza cyberbezpieczeństwo, rozumiane jako wykrywanie, ostrzeganie, reagowanie na incydenty, pozyskiwanie i analiza danych oraz transfer wiedzy.

| Państwowy Instytut Badawczy NASK ul. Kolska 12, Warsaw | +48 22 380 82 00 | www.nask.pl |