Ministerstwo Cyfryzacji

23. Konferencja Miasta w Internecie

Budowanie kompetencji cyberbezpieczeństwa w administracji …

… samorządowej i podmiotach podległych

Robert Kośla

Dyrektor

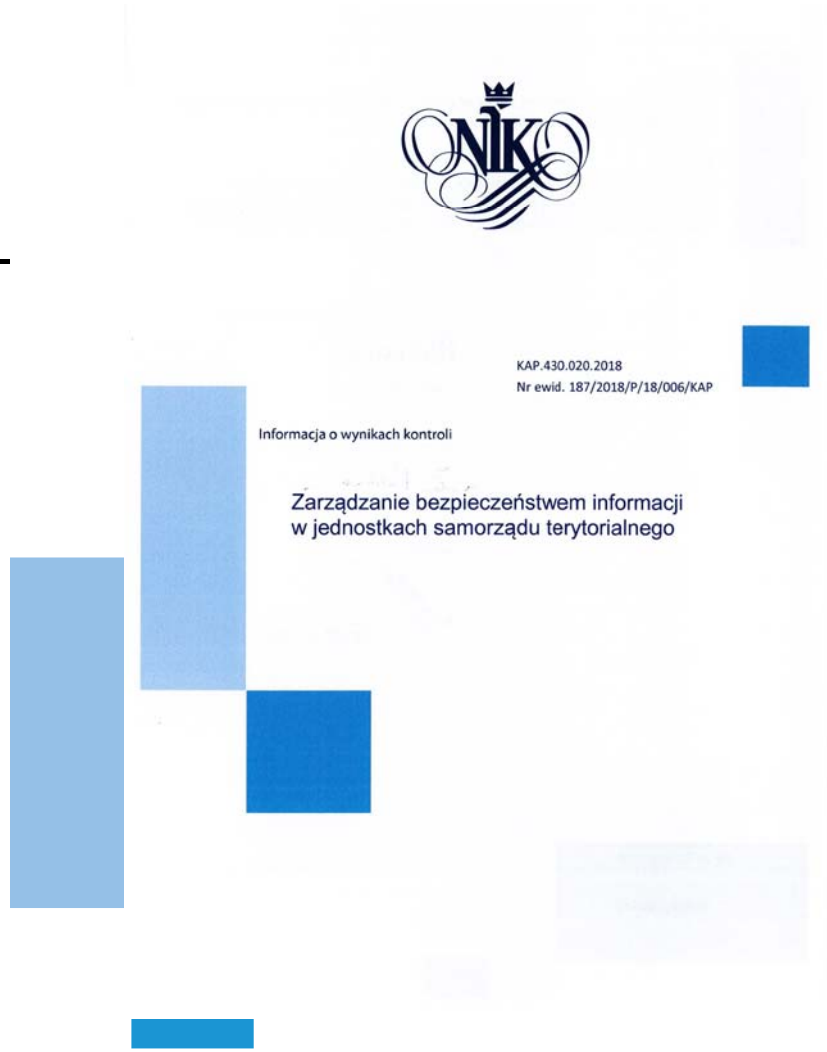
Departament Cyberbezpieczeństwa

Inspiracja do działań ? ☺

Wyniki kontroli Najwyższej Izby Kontroli w zakresie zarządzania bezpieczeństwem informacji w jednostkach samorządu terytorialnego w roku 2018 oraz 2019

„Brak systemowego podejścia do zapewnienia bezpieczeństwa informacji"

- frag. oceny ogólnej NIK



Czy elektroniczne zasoby informacyjne w jednostkach samorządu terytorialnego są właściwie chronione? - NIK

Niezapewnianie **właściwej ochrony** elektronicznych zasobów informacyjnych **przed nieuprawnionym dostępem, przejęciem lub zniszczeniem**

Nieprzeprowadzanie audytów bezpieczeństwa informacji

Nieprowadzenie analiz ryzyka w zakresie bezpieczeństwa

Wykorzystywanie systemów operacyjnych **nieposiadających wsparcia producenta**

Nadawanie **nadmiernych uprawnień** w systemach informatycznych

Brak monitorowania dostępu do systemów informatycznych

Brak odpowiedniego nadzoru nad zdalnym dostępem do zasobów

Brak zabezpieczenia przed **nieautoryzowanym dostępem**

Nieodpowiednie zabezpieczenie **zbiorów danych i infrastruktury informatyczne**j

Brak szkoleń

Diagnoza przyczyn

- **Brak dostatecznej świadomości** wśród osób sprawujących funkcję organu tego, jak ważnym jest problematyka bezpieczeństwa informacji
- Nawet tam gdzie jest świadomość potrzeby ochrony informacji, **występują obiektywne trudności w realizacji niezbędnych przedsięwzięć, powodowane głównie brakami środków finansowych**, a co za tym idzie brakami w dostępie do fachowców z zakresu bezpieczeństwa informacji

Budowanie kompetencji - Zgłaszanie incydentów...

Co to jest incydent, czy, gdzie i jak go zgłosić ?

Obowiązki podmiotów publicznych - wymagania sprzed ustawy o KSC

Rozporządzenie Krajowe Ramy Interoperacyjności:

§ 20. 2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie [realizację] następujących działań:

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących

Obowiązki podmiotów publicznych (w tym JST) z ustawy o Krajowym Systemie Cyberbezpieczeństwa

Wyznaczenie osoby odpowiedzialnej za utrzymanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa i przekazanie do właściwego CSIRT danych tej osoby w terminie 14 dni od dnia jej powołania

Możliwość wyznaczenia przez jednostkę samorządu terytorialnego **jednej osoby dla swoich jednostek organizacyjnych**

Możliwość wyznaczenia przez organ administracji publicznej **jednej osoby dla wszystkich jednostek podległych** lub nadzorowanych przez ten organ

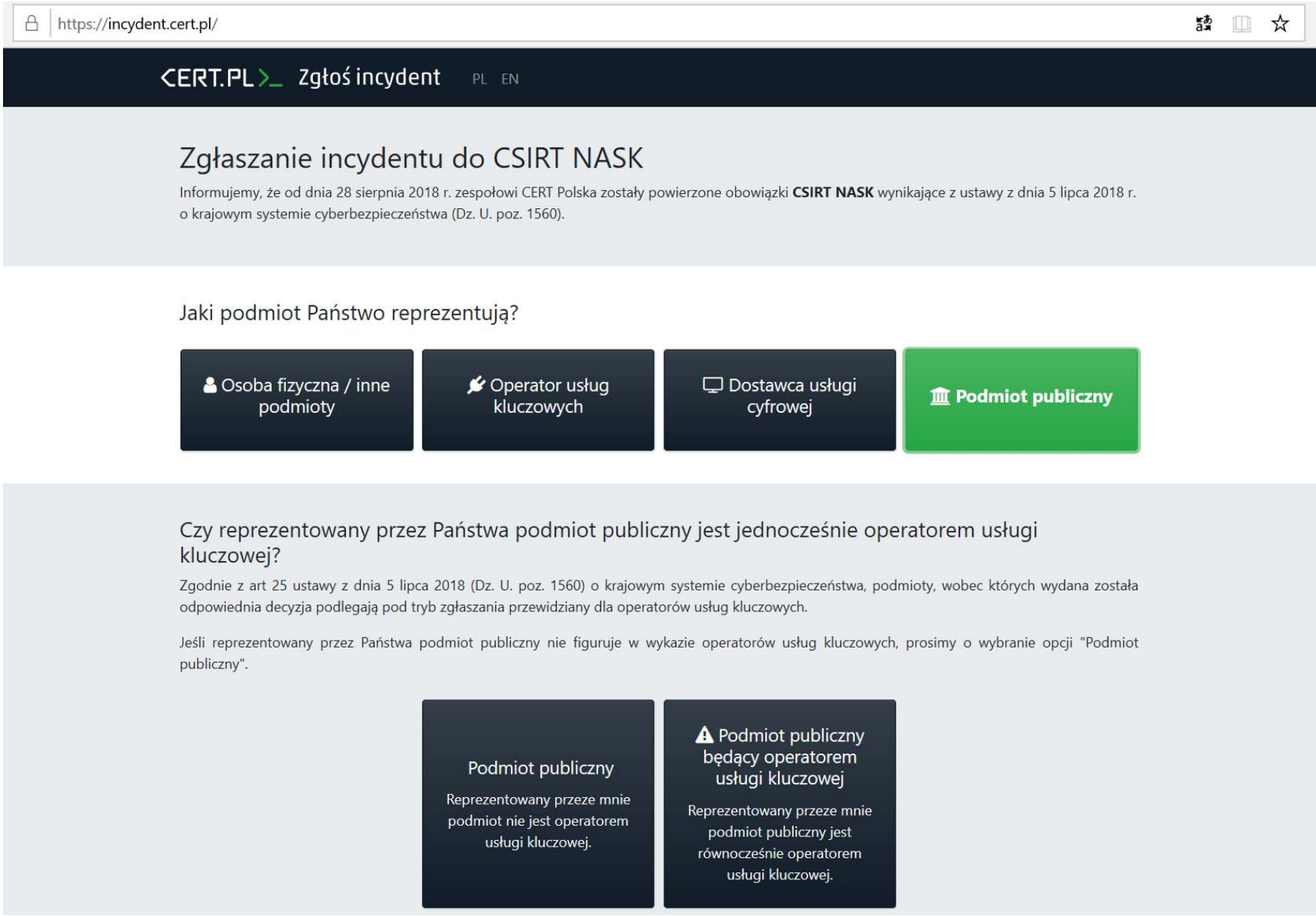
Obowiązki podmiotów publicznych (w tym JST) z ustawy o Krajowym Systemie Cyberbezpieczeństwa

Podmiot publiczny:

- zarządza incydentami
- zgłasza incydent do właściwego CSIRT
- (w terminie: 24 h od momentu wykrycia)
- zapewnia obsługę incydentu
- prowadzi działania edukacyjne wobec użytkowników

JST zgłaszają incydenty do zespołu CSIRT NASK

Zgłaszanie incydentów do CSIRT NASK



Co JST powinny zgłaszać?

incydent – każde zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo

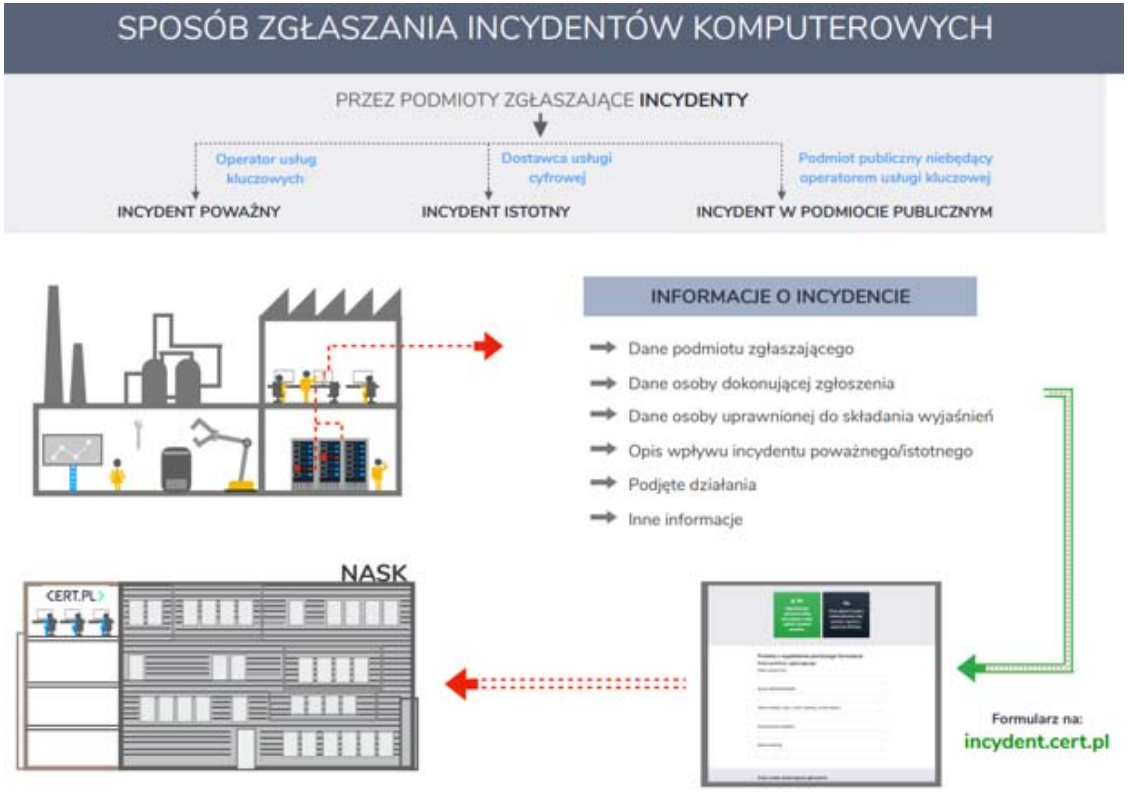
(Nie trzeba zgłaszać, ale można – zachęcamy do tego)

incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny

Zadanie publiczne – brak definicji, w skrócie: zadanie realizowane na podstawie ustawy i dla dobra ogólnego

Obowiązek ustawowy zgłoszenia incydentu

Sposób zgłaszania incydentów w CSIRT NASK



Budowanie kompetencji - Szkolenia...

Co przygotowujemy wspólnie z NASK PIB ?

Budowanie kompetencji w JST – poradniki

Poradniki opracowane przez NASK PIB dostępne na stronie Ministerstwa Cyfryzacji

Poruszane tematy:

- Organizacja KSC
- Zasady zgłaszania incydentów
- Ochrona danych osobowych a cyberbezpieczeństwo

Więcej informacji na www.gov.pl/web/cyfryzacja/edukacja

Grupa Robocza ds. Cyberbezpieczeństwa w MC:

www.gov.pl/web/cyfryzacja/grupa-robocza-ds-cyberbezpieczenstwa

gov.pl Serwis polskiego rządu

Ministerstwo Cyfryzacji

O ministerstwie | Co robimy | Aktualności | Załatw sprawę

Ministerstwo Cyfryzacji / Co robimy / Cyberbezpieczeństwo / Edukacja

Edukacja

Ministerstwo w porozumieniu z Grupą Roboczą ds. Cyberbezpieczeństwa utworzoną w 2018 r. oraz NASK PIB prezentuje poradniki, które przybliżą Państwu problematykę cyberbezpieczeństwa oraz ułatwią wdrażanie obowiązków wynikających z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Ustawa o krajowym systemie cyberbezpieczeństwa wprowadziła nowe zadania i obowiązki zarówno dla przedsiębiorców jak i podmiotów publicznych, w tym jednostek samorządu terytorialnego. Ustawa tworzy ramy prawne, na których oprzemy bezpieczne usługi kluczowe i cyfrowe. Dzięki nim także szeregowi pracownicy oraz zwykli użytkownicy będą mogli czuć się bezpieczniej.

Poniższe poradniki kierujemy do wszystkich grup objętych ustawą.

Poradniki adresowane do **jednostek samorządu terytorialnego** przedstawiają organizację krajowego systemu cyberbezpieczeństwa, zadania i obowiązki podmiotów wchodzących w skład tego systemu oraz procedurę zgłaszania incydentów do Zespołu Reagowania na Incydenty Komputerowe CERT.PL

- Pobierz poradnik dla JST dot. ustawy o krajowym systemie cyberbezpieczeństwa
- Pobierz poradnik dla JST dot. zgłaszania incydentów

Poradnik dla **operatorów usług kluczowych** dotyczący zgłaszania incydentów do Zespołu Reagowania na Incydenty Komputerowe CERT.PL

- Pobierz poradnik dla operatorów usług kluczowych dot. zgłaszania incydentów

W poradniku **„Bezpieczny pracownik w sieci"** przedstawione zostały zagadnienia„ które dotykają każdego pracownika mającego styczność zarówno z dokumentacją tradycyjną, jak i narzędziami IT.

- Pobierz poradnik Bezpieczny pracownik w sieci

Działania podnoszące świadomość o cyberzagrożeniach wśród kadr administracji publicznej w roku 2019

Zadanie zlecone NASK-PIB w ramach dotacji celowej w 2019 r.

W ramach zadania realizowane są dwa podzadania:

1. budowa platformy e-learningowej (e-CTP – Cyber Training Platform) dla kadr administracji publicznej, w tym jednostek samorządu terytorialnego

2. stacjonarne szkolenia dla wybranych jednostek samorządu terytorialnego z obowiązków wynikających z ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwie

Platforma e-learningowa (e-CTP – Cyber Training Platform) podstawowe założenia

- Przygotowana w oparciu o autorskie rozwiązanie e-learningowe wykorzystywane w NASK–PIB
- Przygotowana w modelu Software as a Service (SaaS)
- Udostępniania użytkownikom w trybie on-line

Platforma e-learningowa (e-CTP – Cyber Training Platform)
funkcjonalność merytoryczna

1. **Moduł CyberHigiena** – dedykowany wszystkim pracownikom urzędów dot. rutynowych działań podnoszących bezpieczeństwo online, m.in:
   - używanie odpowiednich haseł oraz ich systematyczna zmiana,
   - unikanie potencjalnie niebezpiecznych witryn,
   - unikanie ściągania plików z podejrzanych źródeł,
   - dbałość o aktualizację oprogramowania itp.

2. **Moduł CyberHigienaPro** – moduł dedykowany kadrze IT zatrudnionej w urzędach nt. zagadnień bezpieczeństwa teleinformatycznego oraz obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa

Platforma e-learningowa (e-CTP – Cyber Training Platform) funkcjonalność użytkowa

- Moduł rejestracyjny użytkowników szkolenia
- Możliwość wyboru odpowiedniego modułu szkoleniowego
- **Możliwość przeprowadzenia testu kontrolnego** po zakończeniu szkolenia
- **Możliwość wygenerowania elektronicznego certyfikatu ukończenia szkolenia**, po pozytywnie ukończonym teście kontrolnym

Platforma e-learningowa (e-CTP – Cyber Training Platform) uruchomienie

- testowanie – jesień 2019 r. w wybranym/chętnym do współpracy urzędzie marszałkowskim
- pełne uruchomienie – 2020 r.

    - Od 2020 r. urzędy będą sukcesywnie zapraszane do skorzystania z platformy, według harmonogramu ustalonego przez MC
    - Planowane jest uruchomienie call center w godz. 8.00-16.00

Bezpośrednie szkolenia kadr odpowiedzialnych za systemy teleinformatyczne

założenia

Cel:

zwiększenie poziomu bezpieczeństwa w organach administracji publicznej poprzez **podnoszenie świadomości i budowanie kompetencji w zakresie cyberbezpieczeństwa wśród pracowników instytucji samorządowych** pod kątem obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa

- 4 spotkania informacyjne (zorganizowane poprzez 4 wybrane / **chętne do współpracy urzędy marszałkowskie**), które obejmą łącznie ok. 400 osób – pracowników urzędów na szczeblu gminy i powiatu, odpowiedzialnych za realizację zadań wynikających z ustawy o krajowym systemie cyberbezpieczeństwa
- Termin realizacji:
  - wrzesień – grudzień 2019 r. - pilotaż w 4 urzędach marszałkowskich
  - 2020 – szkolenia dla wszystkich urzędów marszałkowskich

Bezpośrednie szkolenia kadr odpowiedzialnych za systemy teleinformatyczne

zakres szkoleń

Moduł poświęcony ustawie o krajowym systemie cyberbezpieczeństwa:

- akty prawne
- architektura krajowego systemu cyberbezpieczeństwa
- obowiązki wynikające z ustawy oraz aktów wykonawczych
- współpraca z podmiotami krajowego systemu cyberbezpieczeństwa

Moduł operacyjny:

- rodzaje ataków
- statystyki ataków
- zgłaszanie incydentów
- reagowanie na incydenty
- postępowanie z nielegalnymi treściami

Budowanie kompetencji - Ćwiczenia...

Inspiracja z ćwiczeń administracji rządowej

ĆWICZENIA REAGOWANIA NA INCYDENTY KOMPUTEROWE W ADMINISTRACJI RZĄDOWEJ 2018

➢ Termin ćwiczenia:

27.11.2018 r.

➢ Cel ćwiczenia.

Głównym celem tego ćwiczenia było praktyczne sprawdzenie świadomości o cyberzagrożeniach i znajomości procedur reagowania w przypadku ich wystąpienia, wśród losowo wybranych grup pracowników Urzędów Administracji Rządowej poprzez przeprowadzenie symulowanej nieinwazyjnej akcji phishingowej polegającej na rozesłaniu specjalnie przygotowanych wiadomości email:

Etap 1 – wiadomość z linkiem do quizu dotyczącym rozpoznawania ataków phishingowych - QUIZ;

Etap 2 – wiadomość z linkiem do nowego portalu w domenie m-urzednik.pl;

Etap 3 – wiadomość z linkiem do pobrania specjalnego skanera antywirusowego.

➢ Uczestnicy ćwiczenia

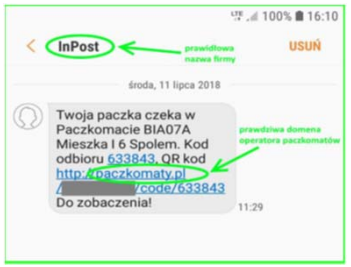
• KPRM	• MEN
• SSC	• MNiSzW
• UKE	• MZ
• MGMiŻŚ	• MS
• MSZ	• MI
• MRiRW	• ME
• MIiR	• MC
• MRPiPS	• MON
• MŚ	• RCB
• MSWiA	• GUS

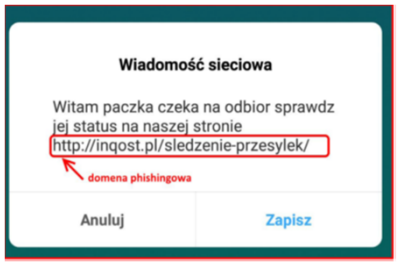
ĆWICZENIA REAGOWANIA NA INCYDENTY KOMPUTEROWE W ADMINISTRACJI RZĄDOWEJ 2018

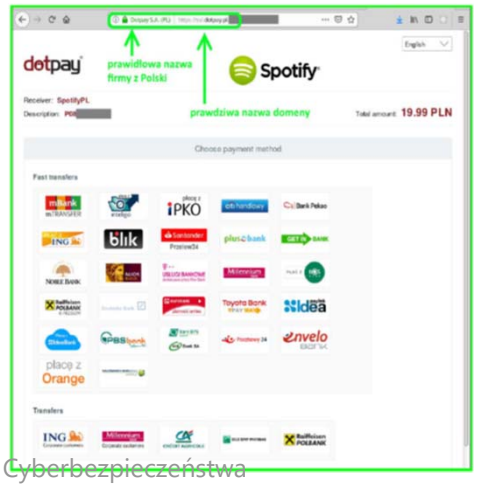
Etap I: Wyniki testu z rozpoznawania wiadomości phishingowych

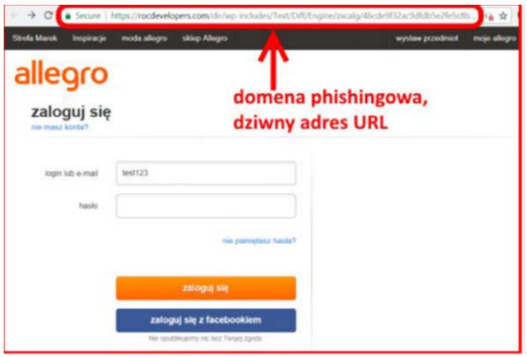
- Maksymalnie punktów: 12
- **Średni wynik: 9.87**
- Mediana: 10

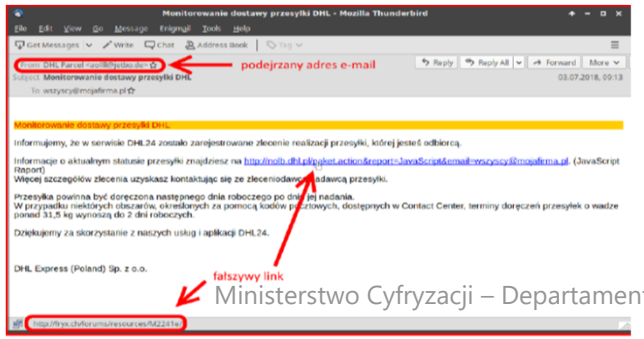
- Odnotowano **681 użytkowników**, którzy rozwiązali test.





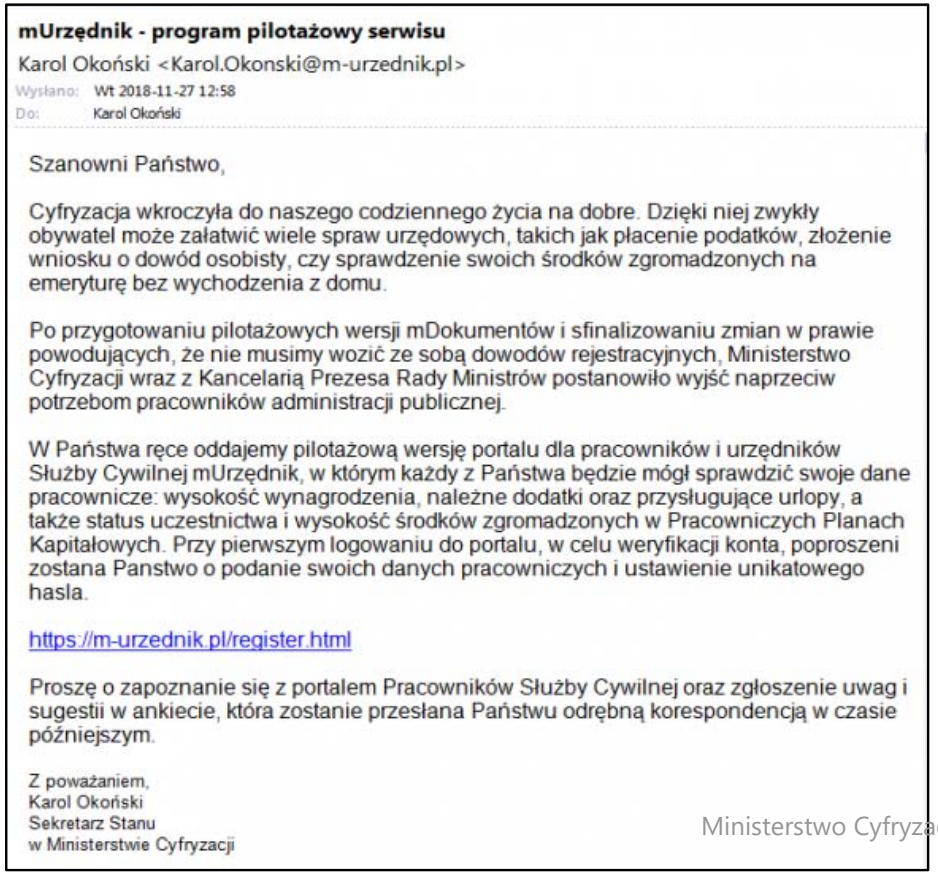






ĆWICZENIA REAGOWANIA NA INCYDENTY KOMPUTEROWE W ADMINISTRACJI RZĄDOWEJ 2018

Etap II: Wyniki po wysłaniu wiadomości z informacją o portalu w domenie m-urzednik.pl.



mUrzędnik - program pilotażowy serwisu

Karol Okoński <Karol.Okonski@m-urzednik.pl>

Wysłano: Wt 2018-11-27 12:58

Do: Karol Okoński

Szanowni Państwo,

Cyfryzacja wkroczyła do naszego codziennego życia na dobre. Dzięki niej zwykły obywatel może załatwić wiele spraw urzędowych, takich jak płacenie podatków, złożenie wniosku o dowód osobisty, czy sprawdzenie swoich środków zgromadzonych na emeryturę bez wychodzenia z domu.

Po przygotowaniu pilotażowych wersji mDokumentów i sfinalizowaniu zmian w prawie powodujących, że nie musimy wozić ze sobą dowodów rejestracyjnych, Ministerstwo Cyfryzacji wraz z Kancelarią Prezesa Rady Ministrów postanowiło wyjść naprzeciw potrzebom pracowników administracji publicznej.

W Państwa ręce oddajemy pilotażową wersję portalu dla pracowników i urzędników Służby Cywilnej mUrzędnik, w którym każdy z Państwa będzie mógł sprawdzić swoje dane pracownicze: wysokość wynagrodzenia, należne dodatki oraz przysługujące urlopy, a także status uczestnictwa i wysokość środków zgromadzonych w Pracowniczych Planach Kapitałowych. Przy pierwszym logowaniu do portalu, w celu weryfikacji konta, poproszeni zostana Panstwo o podanie swoich danych pracowniczych i ustawienie unikatowego hasla.

https://m-urzednik.pl/register.html

Proszę o zapoznanie się z portalem Pracowników Służby Cywilnej oraz zgłoszenie uwag i sugestii w ankiecie, która zostanie przesłana Państwu odrębną korespondencją w czasie późniejszym.

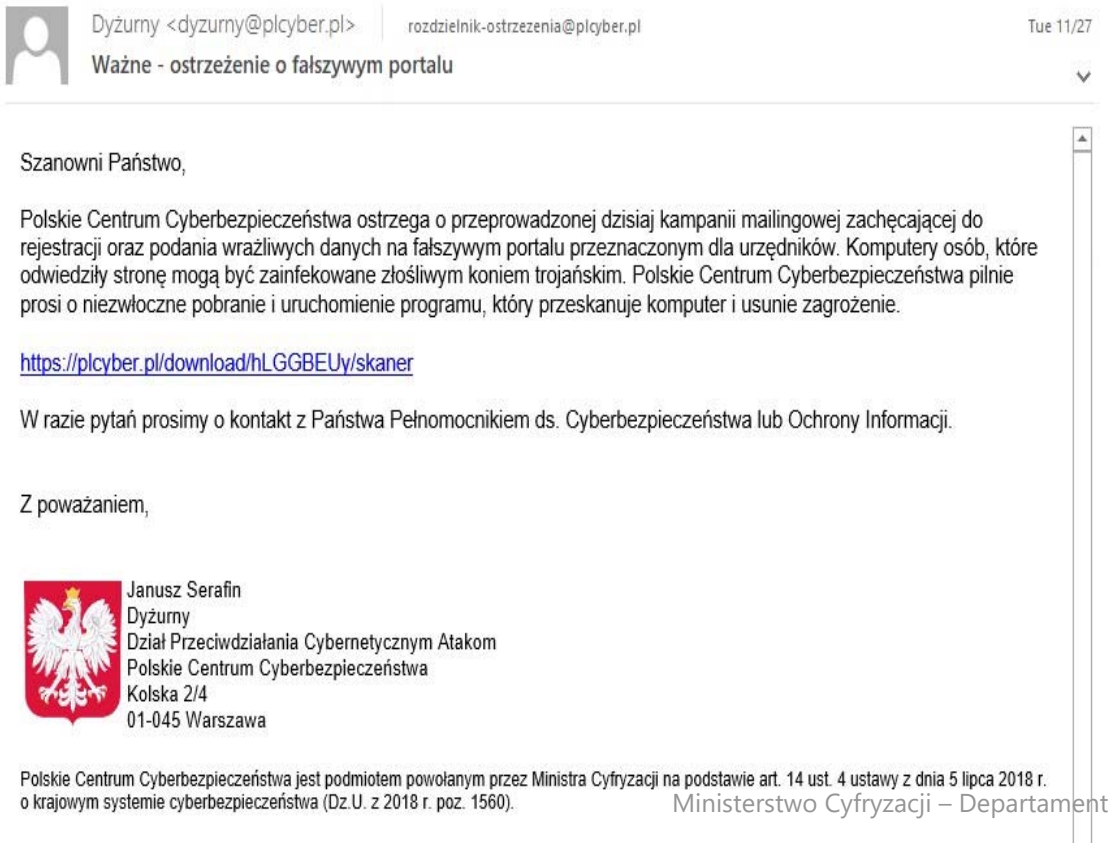
Z poważaniem,
Karol Okoński
Sekretarz Stanu
w Ministerstwie Cyfryzacji

- Podjęte akcje w m-urzędniku

Kliknięcia w link phishingowy	Liczba osób, które zalogowały się lub zarejestrowały się w m-urzędniku
90	28
84	36
41	20
38	5
31	3
26	3
21	4
15	9
13	4
11	3
10	1
8	3
6	4
4	1
3	0
2	0
2	1
405	**125**

ĆWICZENIA REAGOWANIA NA INCYDENTY KOMPUTEROWE W ADMINISTRACJI RZĄDOWEJ 2018

Etap III: Wyniki pobrania fałszywego antywirusa.



Dyżurny <dyzurny@plcyber.pl> rozdzielnik-ostrzezenia@plcyber.pl Tue 11/27

Ważne - ostrzeżenie o fałszywym portalu

Szanowni Państwo,

Polskie Centrum Cyberbezpieczeństwa ostrzega o przeprowadzonej dzisiaj kampanii mailingowej zachęcającej do rejestracji oraz podania wrażliwych danych na fałszywym portalu przeznaczonym dla urzędników. Komputery osób, które odwiedziły stronę mogą być zainfekowane złośliwym koniem trojańskim. Polskie Centrum Cyberbezpieczeństwa pilnie prosi o niezwłoczne pobranie i uruchomienie programu, który przeskanuje komputer i usunie zagrożenie.

https://plcyber.pl/download/hLGGBEUy/skaner

W razie pytań prosimy o kontakt z Państwa Pełnomocnikiem ds. Cyberbezpieczeństwa lub Ochrony Informacji.

Z poważaniem,

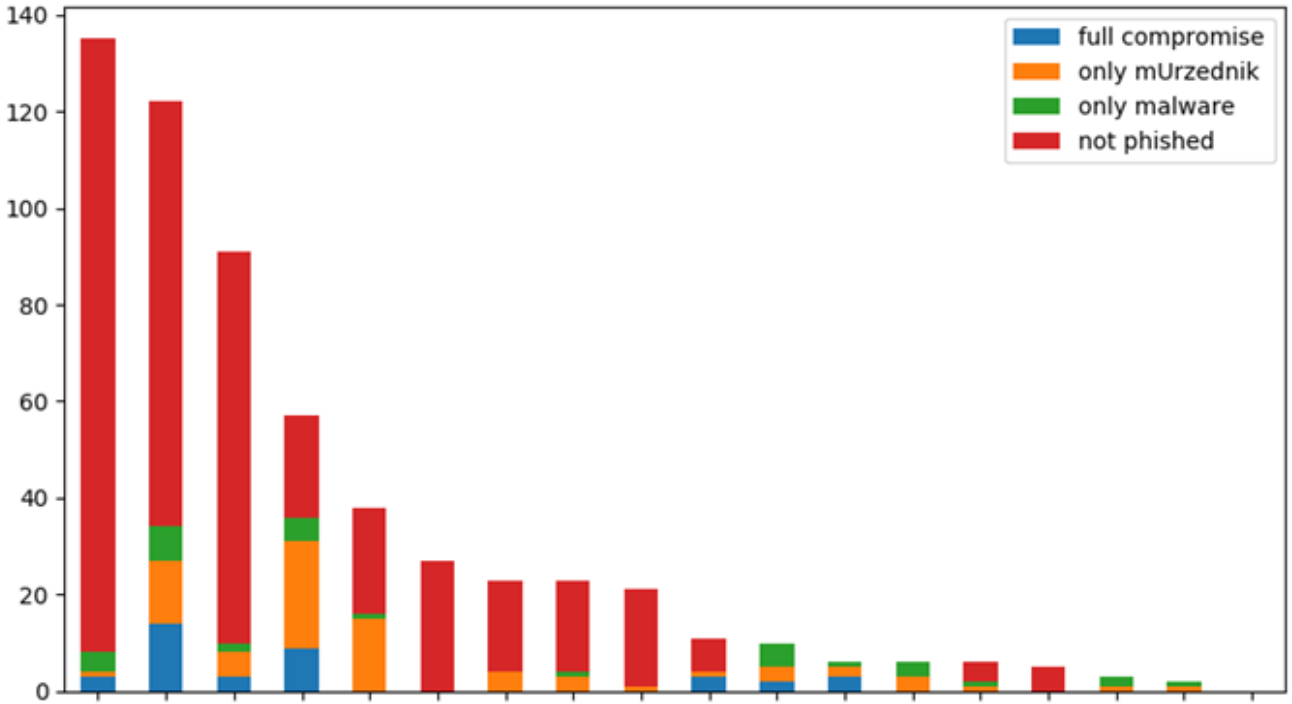
Janusz Serafin
Dyżurny
Dział Przeciwdziałania Cybernetycznym Atakom
Polskie Centrum Cyberbezpieczeństwa
Kolska 2/4
01-045 Warszawa

Polskie Centrum Cyberbezpieczeństwa jest podmiotem powołanym przez Ministra Cyfryzacji na podstawie art. 14 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560).

Liczba pobrań fałszywego antywirusa	Liczba komputerów, na których uruchomiono fałszywego antywirusa
57	0
43	0
39	5
31	4
28	2
14	0
14	3
14	1
10	1
6	0
6	0
2	0
2	1
1	0
0	0
0	0
0	0
265	**17**

ĆWICZENIA REAGOWANIA NA INCYDENTY KOMPUTEROWE W ADMINISTRACJI RZĄDOWEJ 2018

Skuteczność ataków phishingowych w odniesieniu do liczby aktywnych ćwiczących z podziałem na poszczególne podmioty.



- Czerwony kolor oznacza wszystkich zgłoszonych użytkowników.
- Na niebiesko oznaczono udział użytkowników, którzy zarówno podali dane w formularzu rejestracyjnym m-Urzędnika, jak i pobrali złośliwe oprogramowanie.
- Pomarańczowy kolor wskazuje udział pracowników, którzy wyłącznie podali kompletne dane w m-Urzędniku.
- Na zielono oznaczono pracowników, którzy pobrali złośliwe oprogramowanie pomimo braku dokonanej rejestracji na portalu m-Urzędnik.

PLANOWANE ĆWICZENIE CYBERBEZPIECZEŃSTWA W 2019

➢ Krajowe ćwiczenia w zakresie cyberbezpieczeństwa wynikające z Ustawy o Krajowym Systemie Cyberbezpieczeństwa

- Ćwiczenie o zasięgu krajowym z udziałem:
  - CSIRT GOV,
  - CSIRT MON,
  - CSIRT NASK,
  - RCB,
  - Organów Właściwych

➢ Cele ćwiczenia.

- Weryfikacja zdolności operacyjnych i technicznych podmiotów Krajowego Systemu Cyberbezpieczeństwa do działania w sytuacji kryzysowej spowodowanej atakiem teleinformatycznym
- Budowa świadomości w zakresie postępowania w sytuacji kryzysowej wśród organów wchodzących w skład Rządowego Zespołu Zarządzania Kryzysowego

Budowanie Kompetencji
- Partnerstwo dla Cyberbezpieczeństwa

Współpraca NASK PIB – MC – zainteresowanych podmiotów

Partnerstwo dla Cyberbezpieczeństwa - PdC
platforma dobrowolnej współpracy i wymiany doświadczeń oraz informacji o zagrożeniach cyberbezpieczeństwa

- Program Partnerstwa dla Cyberbezpieczeństwa koordynowany przez NASK PIB we współpracy z Ministerstwem Cyfryzacji
- Wpisuje się w realizację zadań z ustawy o Krajowym Systemie Cyberbezpieczeństwa przypisanych CSIRT NASK – art. 26 ust. 6 pkt 2.

- W ramach Programu Partner może:
  - przekazywać do NASK PIB informacje o incydentach
  - informować koordynatora programu o zaobserwowanych zagrożeniach
  - dzielić się wiedzą z zakresu cyberbezpieczeństwa
  - zainicjować powołanie zespołu zadaniowego

- Do chwili obecnej do Programu przystąpiło 50 podmiotów
  - **8 porozumień podpisano z urzędami marszałkowskimi**

https://www.nask.pl/pl/dzialalnosc/cyberbezpieczenstwo/program-partnerstwo-dla/933,Program-Partnerstwo-dla-Cyberbezpieczenstwa.html

Podsumowanie

Podsumowanie - niezbędna praca u podstaw!

1. **Prowadzenie szkoleń i ćwiczeń (w tym dla osób zajmujących kierownicze funkcje)**

2. **Wsparcie w zakresie budowy systemów zarządzania bezpieczeństwem**, w tym standaryzacja dokumentacji normatywnej SZBI, metodyk zarządzania ryzykiem, planowania ciągłości działania, procedur operacyjnych

3. **Standaryzacja bezpieczeństwa** i stałe inwestycje w utrzymanie oprogramowania/urządzeń i usług

4. **Agregacja nadzoru nad cyberbezpieczeństwem** wg. standardów Rządowego Klastra Bezpieczeństwa

5. **Przystąpienie do inicjatywy WIIP** (Wspólnej Infrastruktury Informacyjnej Państwa - hybrydowego środowiska chmur obliczeniowych, chronionego standardem Rządowego Klastra Bezpieczeństwa)

Ministerstwo Cyfryzacji

23. Konferencja Miasta w Internecie

Budowanie kompetencji cyberbezpieczeństwa w administracji samorządowej i podmiotach podległych

Dziękuję za uwagę

Robert Kośla
robert.kosla@mc.gov.pl
sekretariat.dc@mc.gov.pl
Twitter: @robertkosla

Wnioski z kontroli NIK

- **Kontrolowane urzędy nie podejmowały wystarczających działań mających na celu zapobiegania incydentom bezpieczeństwa**. Nie prowadzono okresowych analiz ryzyka w zakresie bezpieczeństwa informacji, a także nie przeprowadzono obowiązkowych audytów w tym zakresie

- **Istnieje potrzeba szerokiego promowania/informowania organów administracji o wymogach w zakresie bezpieczeństwa informacji określonych w rozporządzeniu KRI** oraz ich wpływie na zapewnienie ochrony danych osobowych

NASK IT Szkoła

NASK it szkoła

Korzystaj bezpłatnie

AKTUALNOŚCI | IT SZKOŁA | REJESTRACJA | ZASOBY | KONTAKT

Strona główna > Bezpieczeństwo w sieci

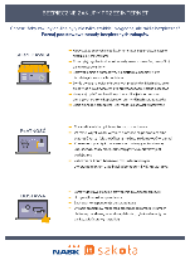
Bezpieczeństwo w Sieci

Bezpieczeństwo w sieci - Infografiki

Przedstawiamy podstawowe zasady cyberhigieny w formie infografik, które zwiększą bezpieczeństwo użytkowników komputerów oraz innych urządzeń mobilnych.

Bezpieczeństwo online

Bezpieczeństwo urządzeń mobilnych

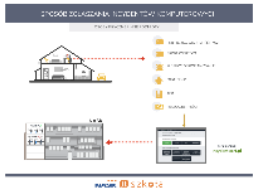


Bezpieczne zakupy przez internet

Bezpieczne korzystanie z chmury

Cyberoszustwa o charakterze finansowym

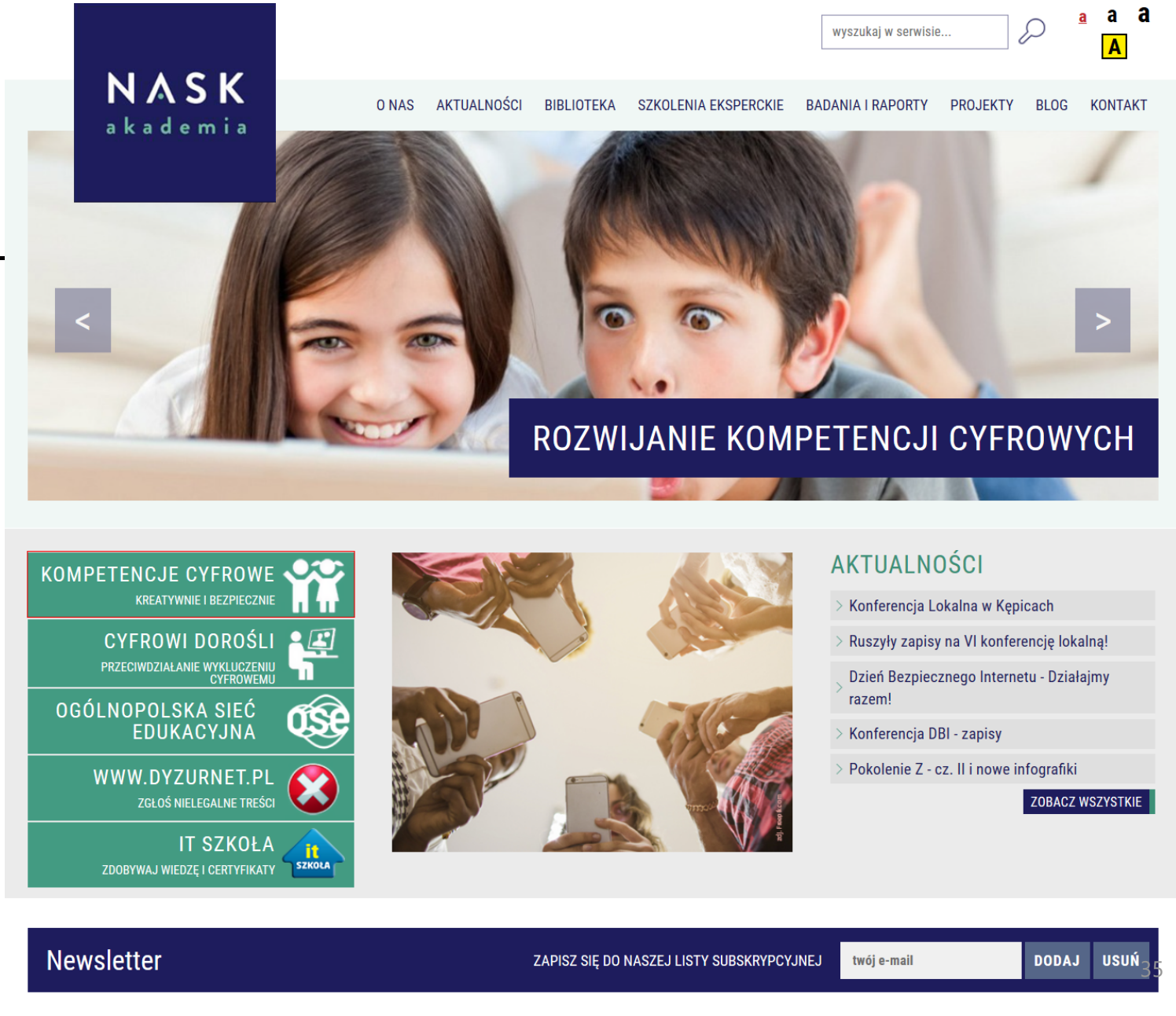
Zgłaszanie incydentów komputerowych - podmioty publiczne



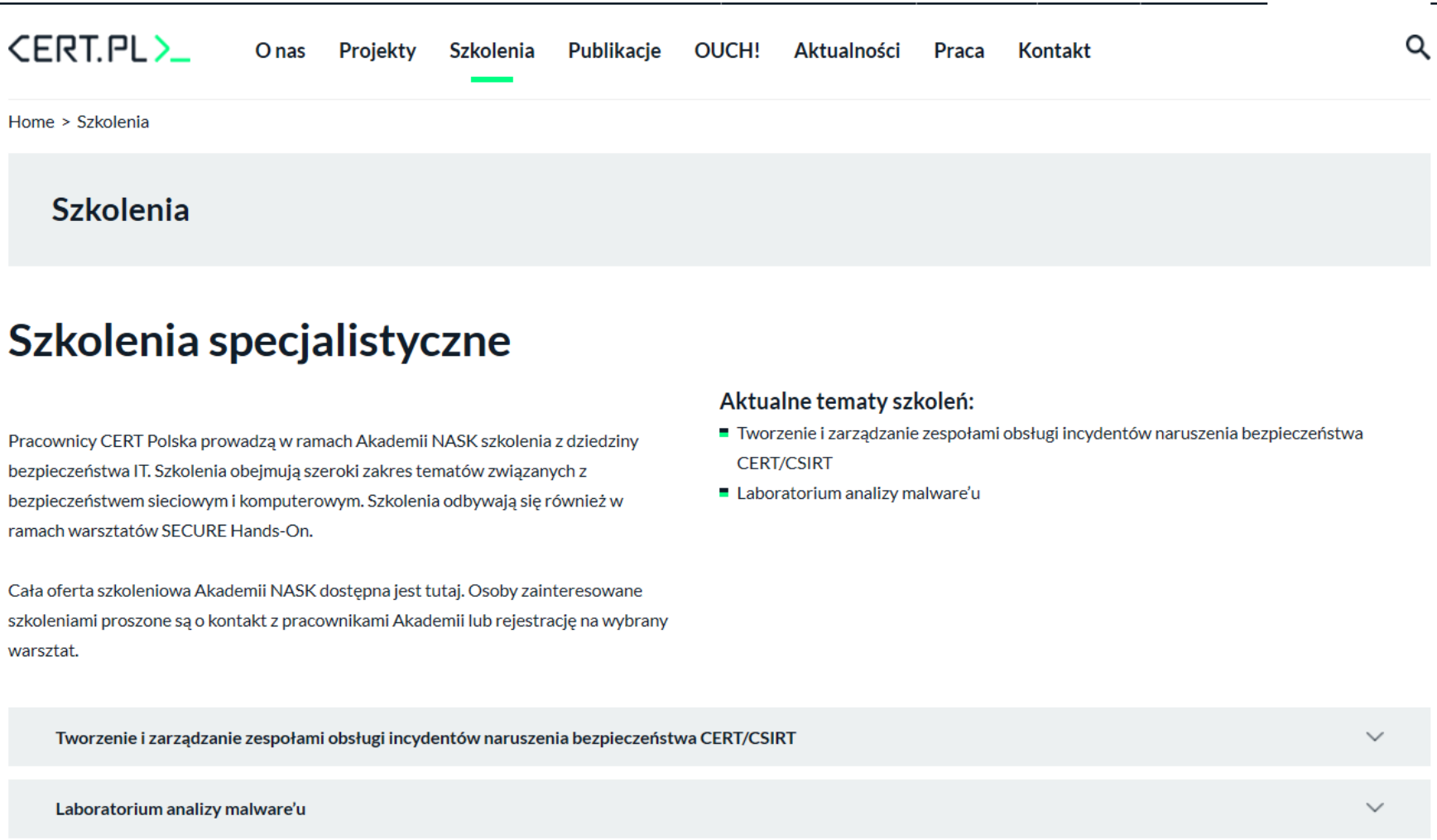
Zgłaszanie incydentów komputerowych - osoby fizyczne/inne podmioty

Publicznie dostępne komputery

NASK Akademia



CSIRT NASK


CERT.PL
O nas
Projekty
Szkolenia
Publikacje
OUCH!
Aktualności
Praca
Kontakt
Home > Szkolenia
Szkolenia
Szkolenia specjalistyczne
Pracownicy CERT Polska prowadzą w ramach Akademii NASK szkolenia z dziedziny bezpieczeństwa IT. Szkolenia obejmują szeroki zakres tematów związanych z bezpieczeństwem sieciowym i komputerowym. Szkolenia odbywają się również w ramach warsztatów SECURE Hands-On.
Cała oferta szkoleniowa Akademii NASK dostępna jest tutaj. Osoby zainteresowane szkoleniami proszone są o kontakt z pracownikami Akademii lub rejestrację na wybrany warsztat.
Aktualne tematy szkoleń:
Tworzenie i zarządzanie zespołami obsługi incydentów naruszenia bezpieczeństwa CERT/CSIRT
Laboratorium analizy malware'u
Tworzenie i zarządzanie zespołami obsługi incydentów naruszenia bezpieczeństwa CERT/CSIRT
Laboratorium analizy malware'u

Platforma e-learningowa (e-CTP – Cyber Training Platform) funkcjonalność administracyjna

- Formularze rejestracyjne dla użytkowników szkoleń
- Moduł do pozyskiwania statystyk
- Moduł zarządzania użytkownikami (określenie ich ról, analityka aktywności itp)