Forum Gospodarcze

TIME

Panel:

Cyberbezpieczeństwo przemysłu cyfrowego

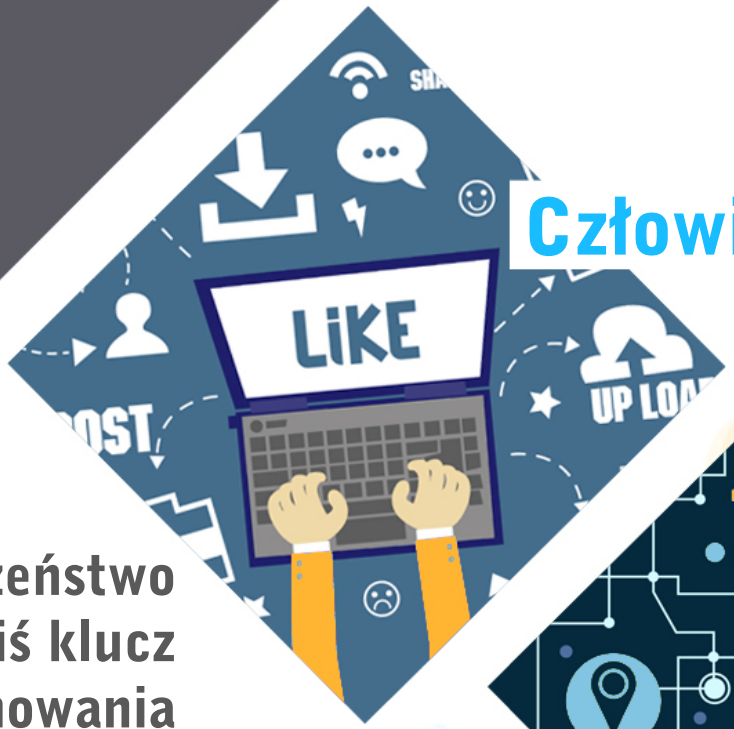
Wprowadzanie:
Wojciech Kamieniecki
NASK

NASK

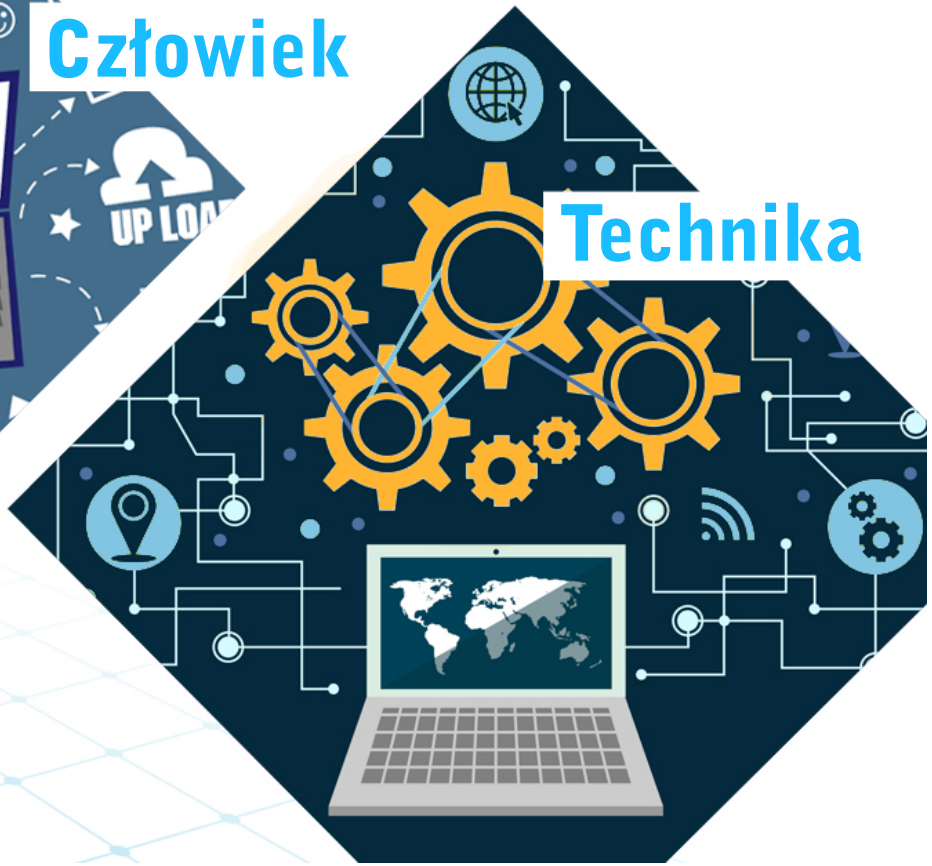
Warszawa, 6 marca 2016 roku

Bezpieczeństwo to nie produkt – to wielowymiarowy proces

Najsłabsze ogniwa cyberobrony:



Człowiek



Technika

Cyberbezpieczeństwo to dziś klucz do funkcjonowania przedsiębiorstw i instytucji

NASK

W sumie w 2015 r.
na całym świecie doszło
do 8,2 mld cyberataków

73% więcej niż rok wcześniej

Istotny wzrost nastąpił także w incydentach obsługiwanych przez NC Cyber w 2016 roku: 1926 incydentów (w 2015: 1456) – na podstawie 7275 zgłoszeń

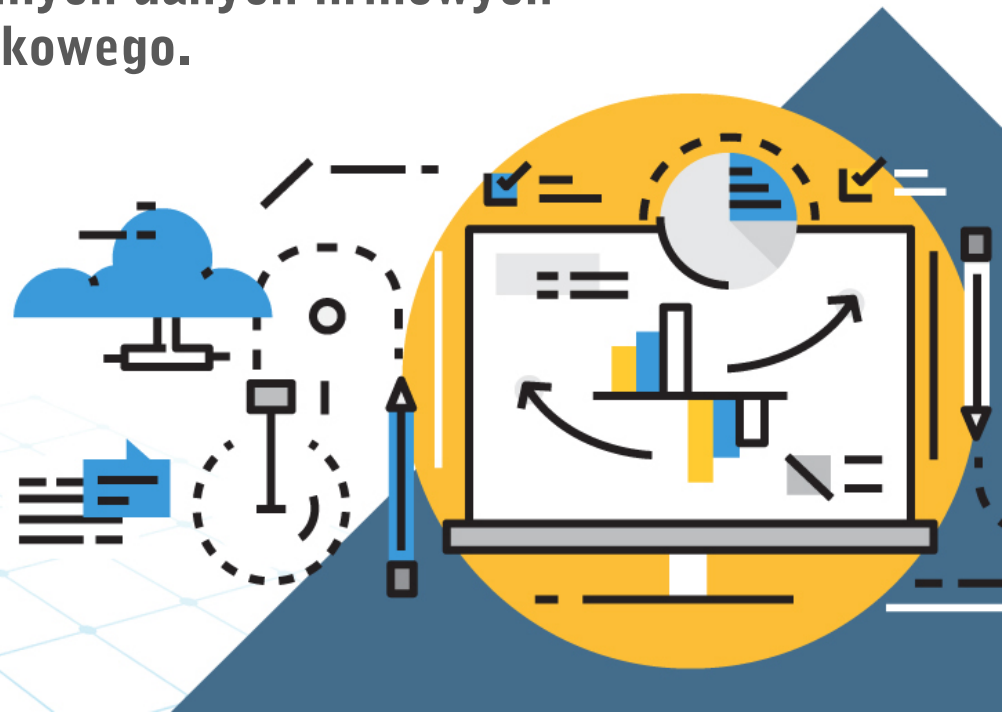
Systemy NC Cyber do automatycznej analizy malware zidentyfikowały 3344 prawdopodobnych adresów serwerów zarządzania botnetami na świecie.

NASK

Potrzeba ochrony przed **e-terrorem** jest coraz bardziej paląca.

Pod obstrzałem są **banki, administracja publiczna, indywidualni użytkownicy** sieci, a przede wszystkim serwery **przedsiębiorstw.**

Technologie mobilne i internet rzeczy → jesteśmy podłączeni do sieci wieloma nitkami przez cały czas → to ułatwia kradzież tożsamości, cennych danych firmowych czy środków z konta bankowego.



NASK

Co jest więc ważne ?

WIEDZA

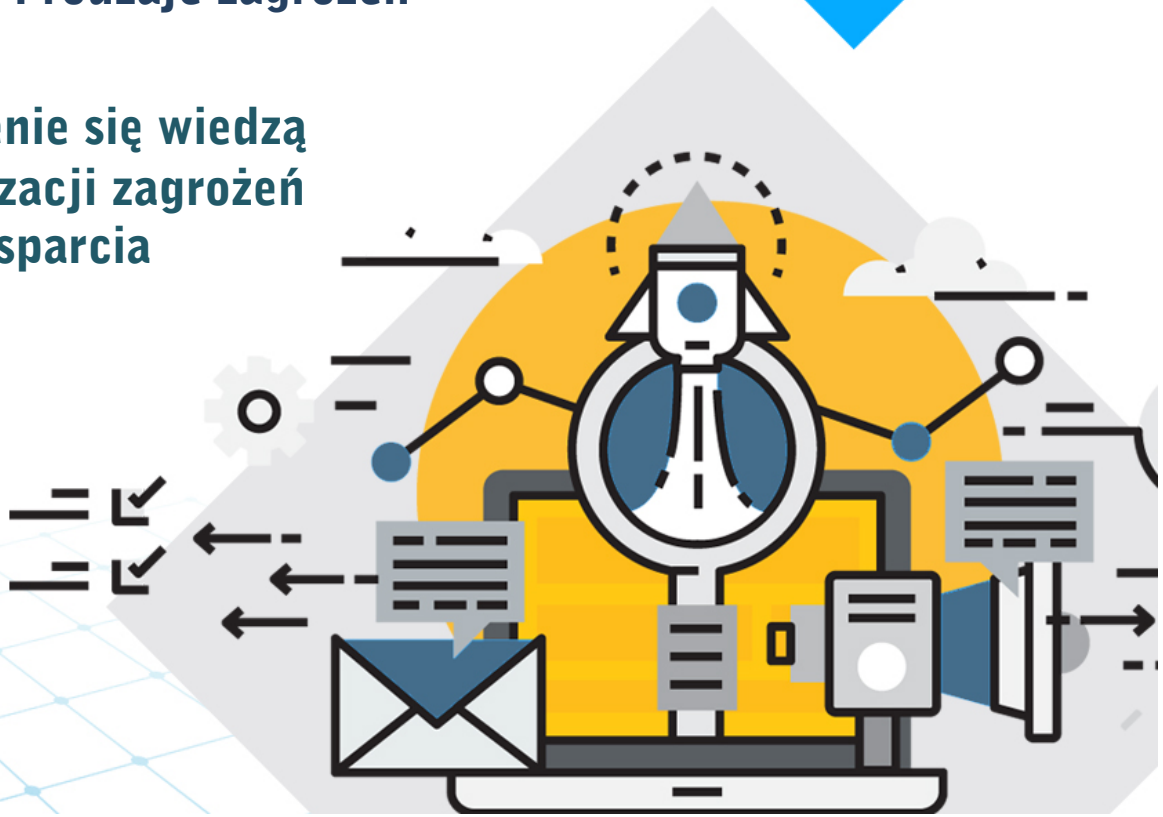
monitorowanie, wymiana informacji i edukacja społeczna, procedury

ROZWÓJ

prace B+R, ciągłe doskonalenie infrastruktury, – zmieniają się wektory ataków i rodzaje zagrożeń

WSPÓŁPRACA

zaufanie i dzielenie się wiedzą w celu minimalizacji zagrożeń i uzyskiwaniu wsparcia



NASK

Co należy robić ?

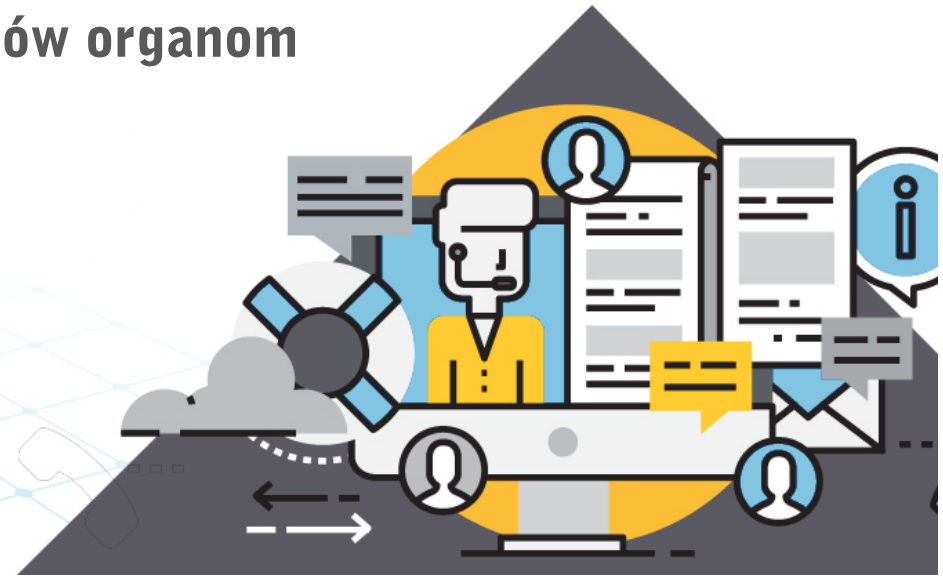
- korzystać z nowoczesnych rozwiązań (np.: model chmurowy, SAAS - security as a service, platforma n6
- dostosowywać rozwiązania do wielkości i możliwości podmiotu oraz trendów zagrożeń
- budować modele współpracy z partnerami

NASK

Jak współdziałać?

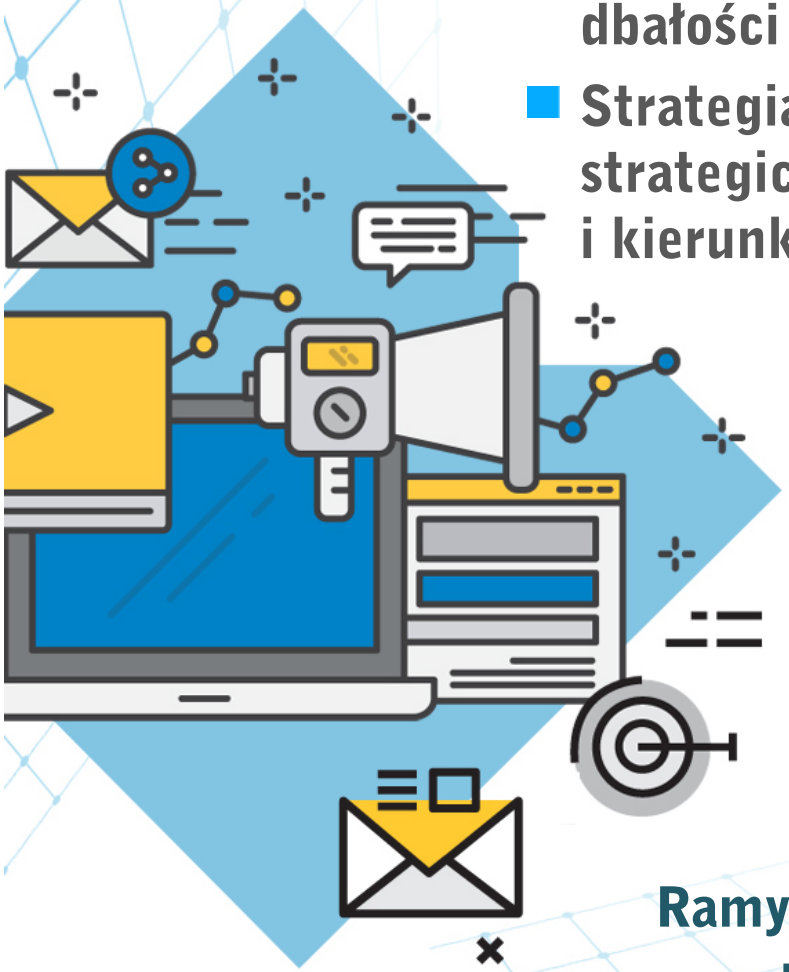
Współpraca pomiędzy sektorem prywatnym a publicznym to kluczowy filar w walce z cyberprzestępczością

- wymiana informacji o incydentach
- dzielenie się wiedzą w sposób poufny i chroniący interesy ofiar ataków
- dostarczanie dowodów organom ścigania



NASK

Jakie otoczenie instytucjonalno-prawne?



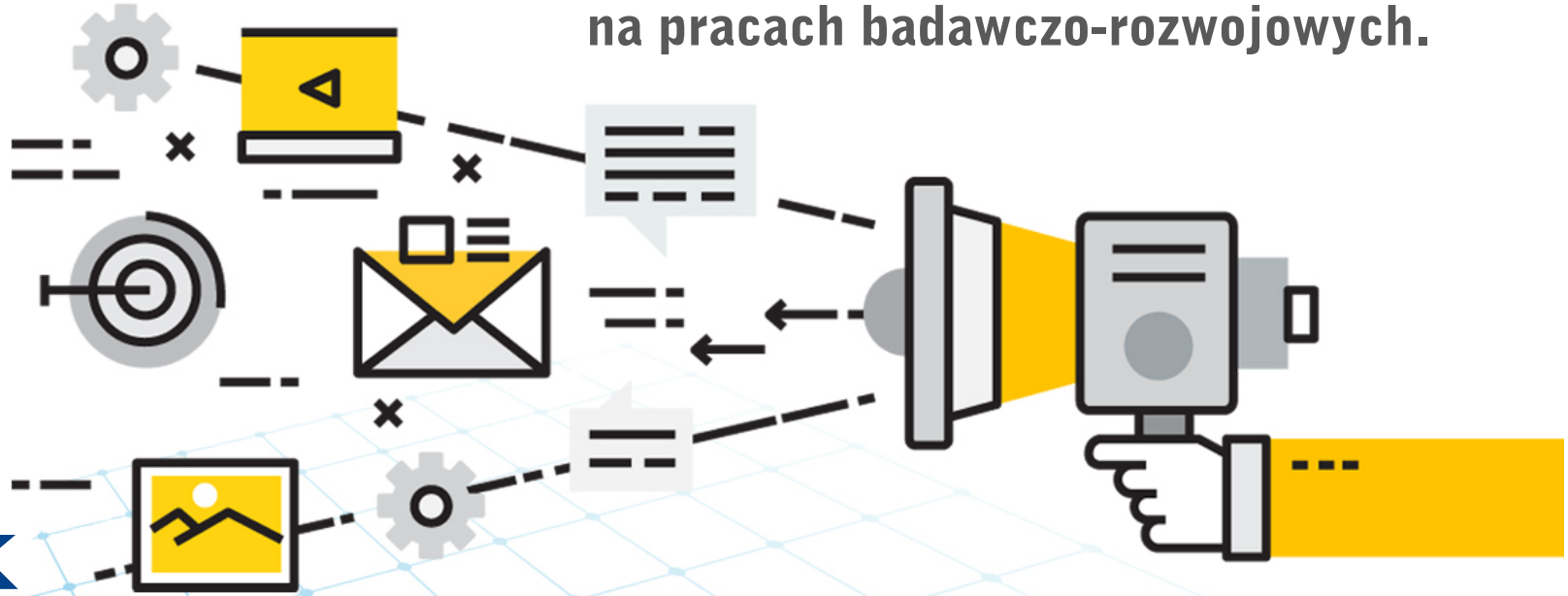
- **Nowe regulacje, w tym unijna dyrektywa NIS, nakładają na przedsiębiorców obowiązek większej dbałości o bezpieczeństwo cyfrowe.**
- **Strategia Cyberbezpieczeństwa RP wskazuje cele strategiczne i operacyjne, ramy organizacyjne i kierunki działań – m.in.:**
  - rozbudowa struktur zajmujących się cyberbezpieczeństwem na poziomie operacyjnym, w tym Narodowego Centrum Cyberbezpieczeństwa (NCC), CSIRT Narodowego, sektorowych zespołów reagowania na incydenty (CSIRT sektorowe), centrów wymiany i analizy informacji.
  - potrzeba umocowania kompetencyjnego na poziomie ustawy odpowiednich struktur, w tym NCC oraz CSIRT Narodowego.

Ramy prawne, technologia oraz współpraca biznesu, nauki i administracji to dopiero połowa sukcesu w walce z e-terroryzmem.

NASK

Co jest potrzebne do budowy aktywnej obrony przedsiębiorstw?

- procedury
- edukacja społeczna
- koordynacja, monitoring i wymiana wiedzy
- doskonalenie technologii
- współpraca partnerami i specjalistami, wdrażanie niestandardowych, i innowacyjnych rozwiązań opartych, na pracach badawczo-rozwojowych.



NASK

Dziękuję za uwagę
i zapraszam do dyskusji

NASK