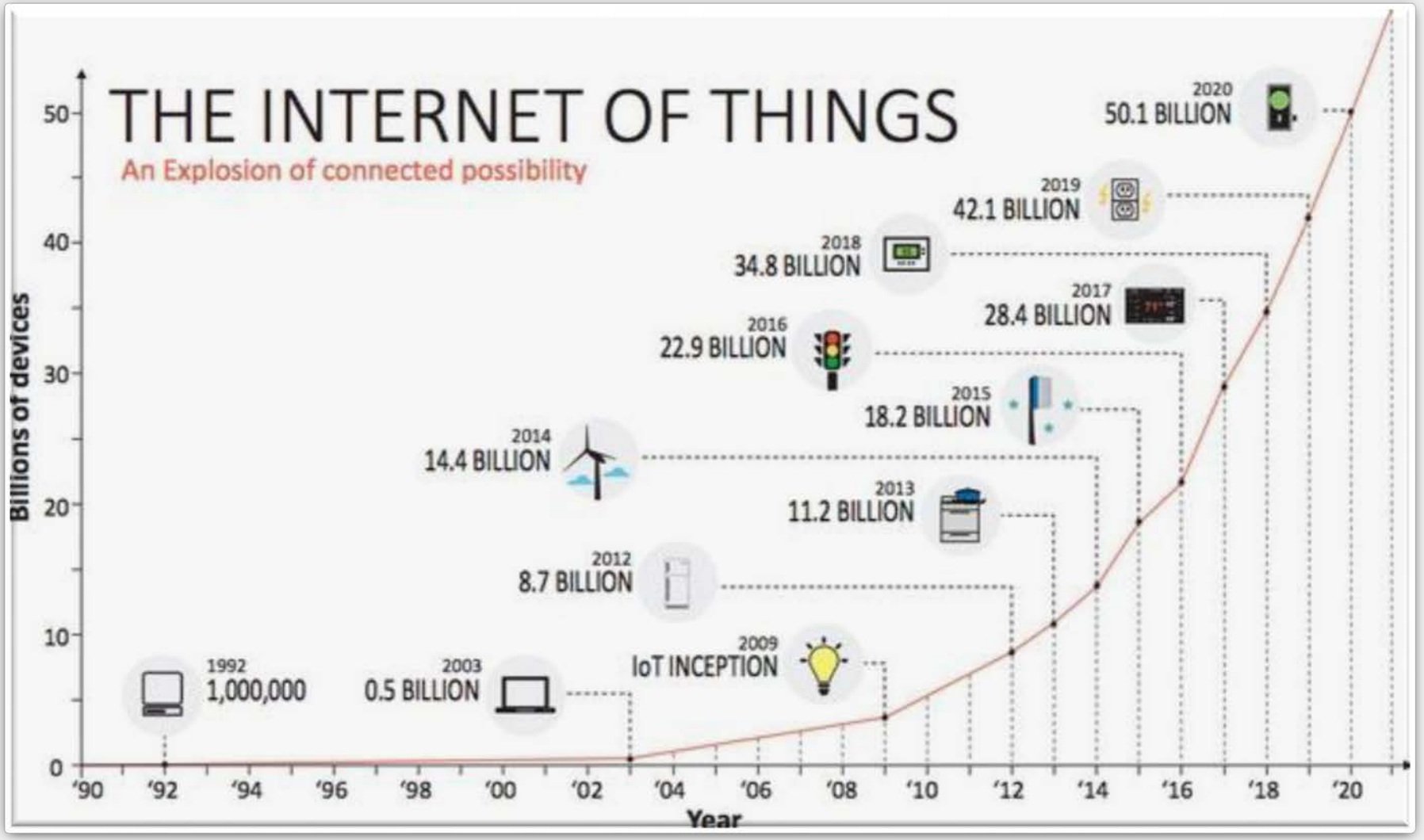
DWUDZIESTE CZWARTE
FORUM
TELEINFORMATYKI®

Wdrażanie rozwiązań Internetu Rzeczy na potrzeby cyfryzacji państwa – czy stać nas na rezygnację z bezpieczeństwa?

mgr inż. Tomasz MAZURKIEWICZ
Wojskowa Akademia Techniczna
tomasz.mazurkiewicz@wat.edu.pl

Internet rzeczy - wprowadzenie



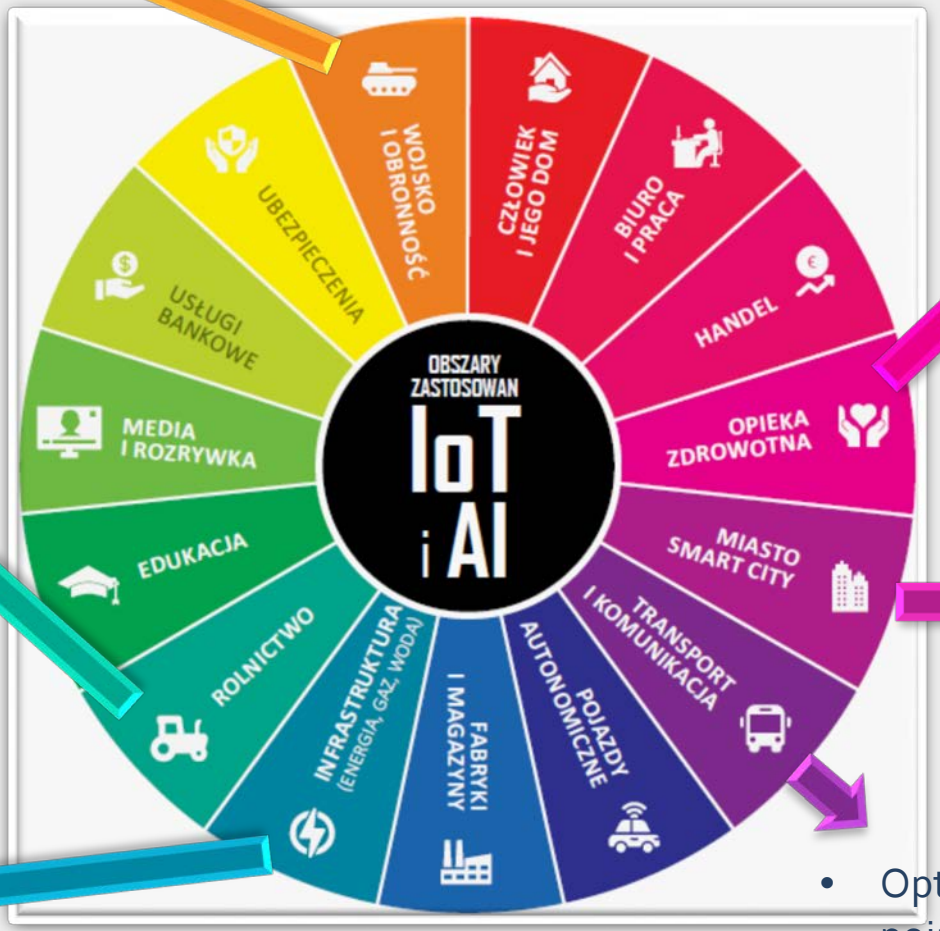
fot.: http://drrajivdesaimd.com/?p=8841

Internet rzeczy - zastosowania

- Projekt **TYTAN**

- Monitorowanie stanu zanieczyszczenia powietrza i wody,
- Monitorowanie poziomu wód gruntowych,
- Monitorowanie wilgotności gleby (np. w okresie susz).

- Wsparcie procesu zarządzania dostawami wody (np. inspekcja zdatności wody do picia),
- Analiza zużycia wody, prądu i gazu przez użytkowników końcowych i optymalizacja ich przesyłu.



fot.: raport Instytutu Sobieskiego "Internet of Things (IoT) i Artificial Intelligence (AI) w Polsce. Jak wykorzystać rewolucję technologiczną Internetu Rzeczy i Sztucznej Inteligencji w rozwoju Polski."

- Monitorowanie stanu pacjenta 24/7 => dokładniejsza i skuteczniejsza diagnoza => skrócenie czasu hospitalizacji

- Efektywne alarmowanie służb,
- Monitorowanie miasta z wykorzystaniem algorytmów rozpoznawania zachowań
- Zarządzanie gospodarką odpadami

- Optymalizacja ruchu pojazdów,
- Inteligentne sterowanie sygnalizacją świetlną,
- Informowanie o wolnych miejscach parkingowych

GDZIE JEST HACZYK?!

70% podłączonych do sieci urządzeń IoT nie spełnia fundamentalnych wymogów bezpieczeństwa

(PWC, *Managing cyb* *ected world*, 2015)

fot.: pixabay

Internet Rzeczy - zagrożenia

„Według ekspertów cyberbezpieczeństwa zatrzymanie używania przez hakerów Internetu Rzeczy do przeprowadzania ataków cybernetycznych będzie **bardzo trudne, jeżeli nie niemożliwie**.

(...)

Oprócz tego, że w niektórych **tańszych urządzeniach** po prostu **brakuje odpowiednich warstw zabezpieczeń**, to rzadko kiedy hasła domyślne są zmieniane. Podobnie nieczęsto występuje proces **aktualizacji** tych urządzeń.

(...)

Internet Rzeczy nie jest bezpieczny, a znakomita **większość tych urządzeń jest produkowana w Chinach** i potem sprzedawana w głównej mierze na rynek amerykański.”

Źródło: Cyberdefence24.pl

Internet Rzeczy - zagrożenia

Login	Hasło	Login	Hasło	Login	Hasło
666666	666666	guest	guest	root	jvbzd
888888	888888	mother	fucker	root	klv123
admin	(none)	root	(none)	root	klv1234
admin	1111	root	00000000	root	pass
admin	1111111	root	1111	root	password
admin	1234	root	1234	root	realtek
admin	12345	root	12345	root	root
admin	123456	root	123456	root	system
admin	54321	root	54321	root	user
admin	7ujMkooadmin	root	666666	root	vizxv
admin	admin	root	7ujMkooadmin	root	xc3511
admin	admin1234	root	7ujMkoovizxv	root	xmhdipc
admin	meinsm	root	888888	root	zlxx.
admin	pass	root	admin	root	Zte521
admin	password	root	anko	service	service
admin	smcadmin	root	default	supervisor	supervisor
admin1	password	root	dreambox	support	support
Administrator	1234	root	hi3518	tech	tech
Administrator	admin	root	ikwb	ubnt	ubnt
guest	12345	root	juantech	user	user

Źródło: Cluley G., These 60 dumb passwords can hijack over 500000 IoT devices into the Mirai botnet, 2016

Internet Rzeczy – zagrożenia proceduralne

Ogłoszenia w BZP – rok 2016 (po nowelizacji)

Kryterium	Liczba / odsetek postępowań							
	roboty budowlane		dostawy		usługi		Ogółem	
Cena jako jedyne kryterium	256	3%	3 058	22%	1 072	10%	4 386	13%
Cena i inne kryteria	9 907	97%	10 585	78%	9 650	90%	30 142	87%
Ogółem	**10 163**	**100%**	**13 643**	**100%**	**10 722**	**100%**	**34 528**	**100%**

Kryteria po wejściu w życie nowelizacji z dnia 22 czerwca 2016 r. (2016 r. i I kwartał 2017 r.)

Kryterium	Liczba	Odsetek postępowań / zadań	Waga kryterium [%]		
			Minimum	Średnia	Maksimum
termin realizacji / czas dostawy	1 429	30%	1	22	97
gwarancja / rękojmia (termin, warunki itp.)	1 194	25%	2	20	60
płatności (warunki, terminy itp.)	500	10%	1	22	40
jakość / funkcjonalność / parametry techniczne (itp.)	895	42%	1	29	60
wiedza / doświadczenie	876		4	26	75
czas reakcji	219		3	22	40
cena	**4 772**	**100%**	3	64%	99

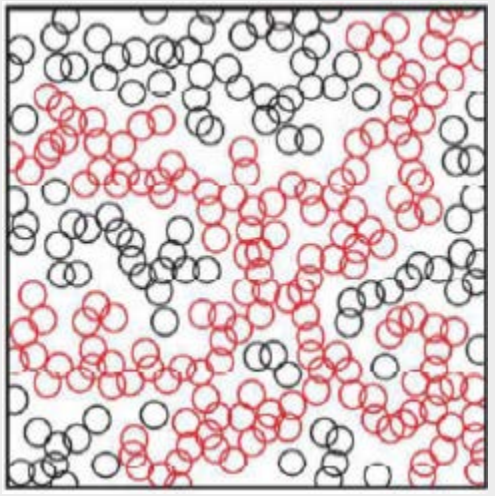
fot. Urząd Zamówień Publicznych, Raport dotyczący kryteriów oceny ofert - wpływ zmian wprowadzonych nowelizacjami ustawy Prawo zamówień publicznych z dnia 29 sierpnia 2014 r. i z dnia 22 czerwca 2016 r. na stosowanie pozacenowych kryteriów ofert w postępowaniach o zamówienie publiczne, 2017

Internet Rzeczy – zagrożenia zewnętrzne

- Liczba ataków – bardzo duża,
- Rodzaje zagrożeń:

–Ataki na pojedyncze urządzenie IoT

–Ataki na sieć urządzeń IoT



– Ataki z wykorzystaniem urządzeń IoT

fot. (l) https://twitter.com/kaspersky (ś) Ronen E. (et al.), *IoT Goes Nuclear: Creating a ZigBee Chain Reaction*, Cryptology ePrint Archive: Report 2016/1047 (p) https://krebsonsecurity.com/2018/05/study-attack-on-krebsonsecurity-cost-iot-device-owners-323k/

Atak typu DDoS z wykorzystaniem botnetu urządzeń IoT na stronę KrebsOnSecurity.com w 2016 roku

- **Skutek**: strona niedostępna przez kilka dni
- **Koszt ochrony przed atakiem tego typu**: **200k $/rok**
- **Koszt ataku** (z punktu widzenia właścicieli wykorzystanych urządzeń): **~320k $**
- **Koszt ataku** (z punktu widzenia atakującego): **~0 $**

Podsumowanie

Do 2020 ataki na urządzenia IoT stanowić będą **25%** wszystkich ataków cybernetycznych.

Aspekt bezpieczeństwa przy wdrażaniu Internetu Rzeczy **nie może** być ignorowany i wymaga szczególnej uwagi oraz kompleksowego planowania, celem uniknięcia przykrych konsekwencji.