Możliwości rozwoju branży ICT dzięki rozpowszechnianiu koncepcji Smart City

Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Mirosław Hajder

Zawartość prezentacji

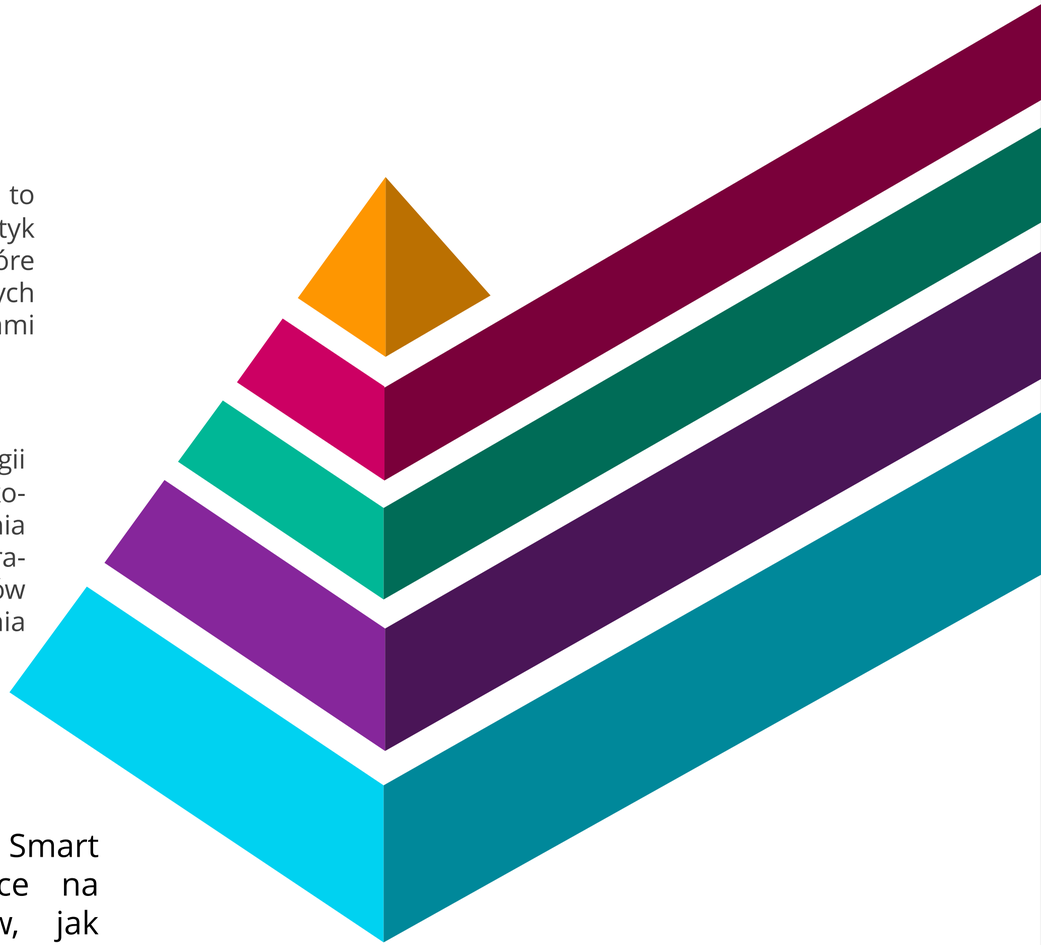
- Pojęcia cyberbezpieczeństwa i Smart City
- Zasięg działań cyberprzestępczych
- Hakerzy i ich motywacje
- Zagrożenia bezpieczeństwa w Smart City
- Cybeprzestępczość a Smart City
- Podsumowanie

Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Cyberbezpieczeństwo a Smart City

Cyberbezpieczeństwo to zestaw procesów, najlepszych praktyk i rozwiązań technologicznych, które ułatwiają chronienie krytycznych systemów i sieci przed atakami cyfrowymi.

Smart City zbiór technologii informacyjno-komunikacyjnych wykorzystywanych w celu zwiększenia interaktywności i wydajności infrastruktury miejskiej i jej komponentów składowych, a także do podniesienia świadomości mieszkańców.



Pomiędzy Cyberbezpieczeństwem a Smart City istnieje powiązanie, wpływające na wzajemne relacje obu podmiotów, jak również na każdy z nich oddzielnie

Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Definicja przestępstwa cybernetycznego

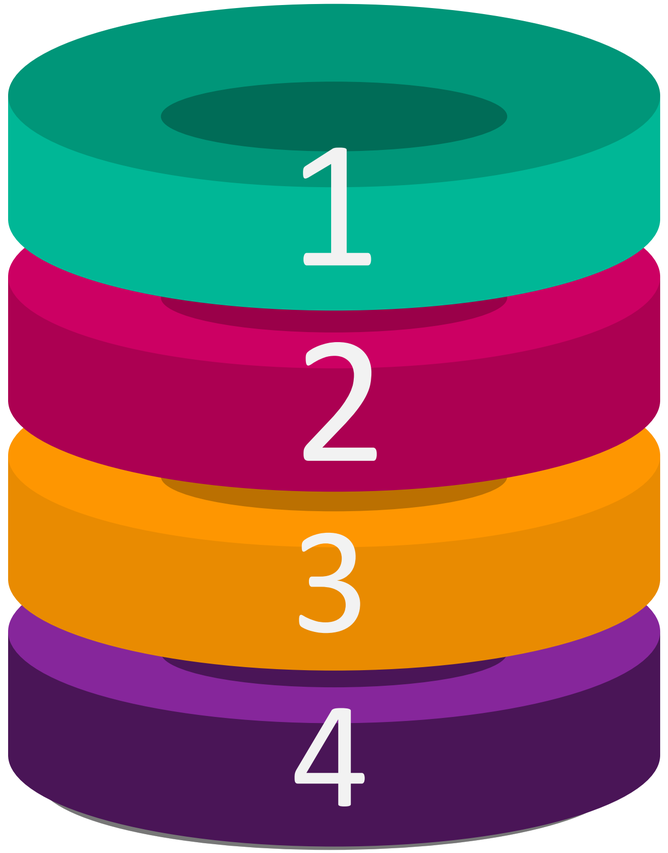
Niestety obecnie brakuje ujednoliconej międzynarodowej terminologii dotyczącej przestępczości cybernetycznej, również w różnych krajach funkcjonują różne uwarunkowania prawne. Podstawy terminologiczne cyberprzestępczości można opisać za pomocą następujących bazowych terminów:

Cyberprzestępczość - zbiór przestępstw popełnianych w *cyberprzestrzeni* za pomocą lub za pośrednictwem systemów lub sieci komputerowych, a także innych środków dostępu do niej, z zastosowaniem komputerów lub sieci, a także przeciwko systemom, sieciom i danym komputerowym;

Cyberprzestępczość odnosi się do każdego przestępstwa popełnionego przy użyciu dowolnych metod i środków tworzenia, przetwarzania, przesyłania danych komputerowych;

Termin *cyberprzestępczość* jest często używany zamiennie z terminem **przestępczość komputerowa**. Należy pamiętać jednak, że termin *cyberprzestępczość* jest szerszy od terminu *przestępczość komputerowa*, ponieważ dotyczy on przestępstw popełnianych w przestrzeni informacyjnej;

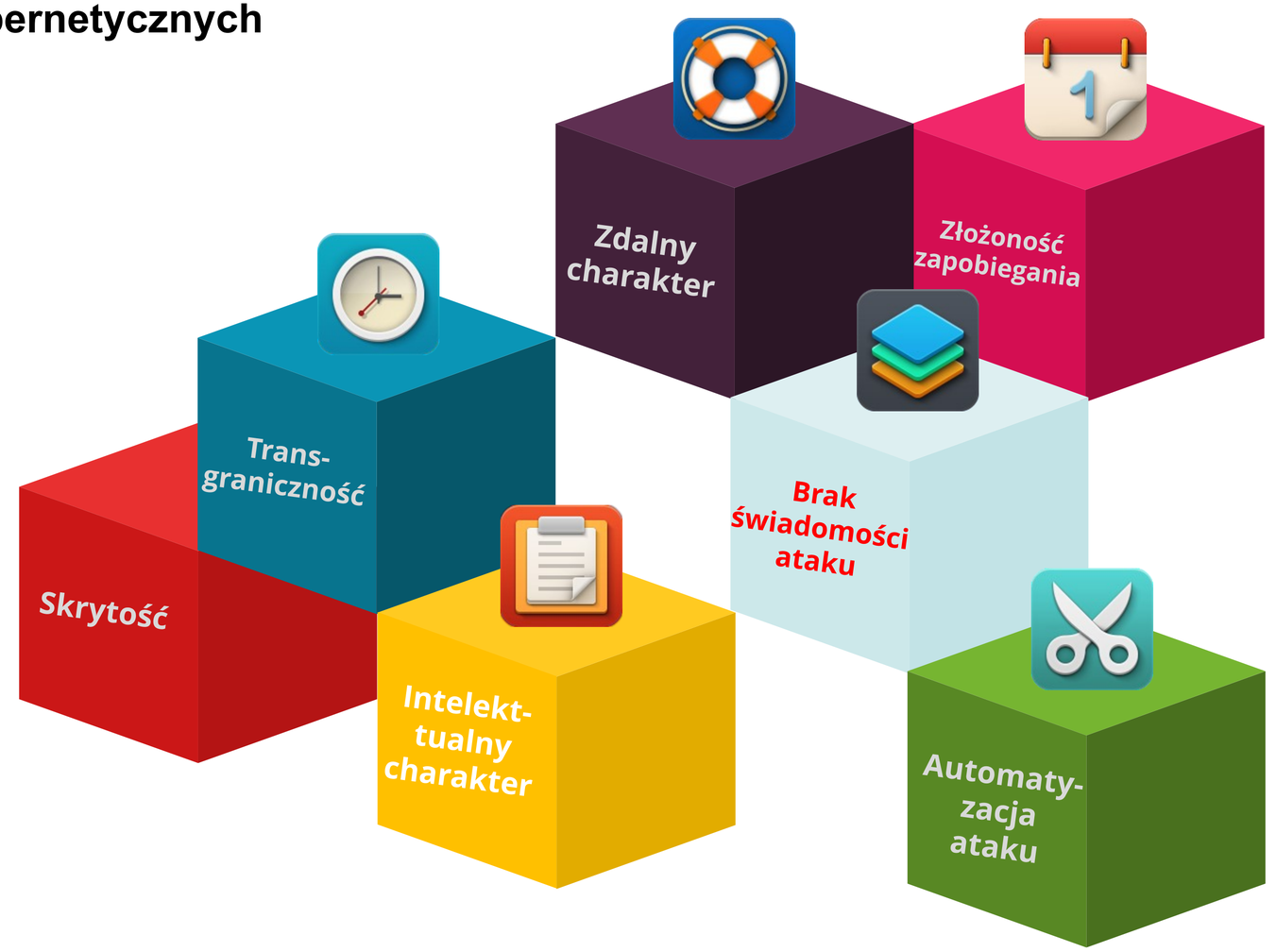
Najczęściej uważa się, że ***cyberprzestępczość*** to przestępczość związana zarówno
z wykorzystaniem komputerów, jak i technologii informatycznych lokalnie bądź w sieciach rozległych.



Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

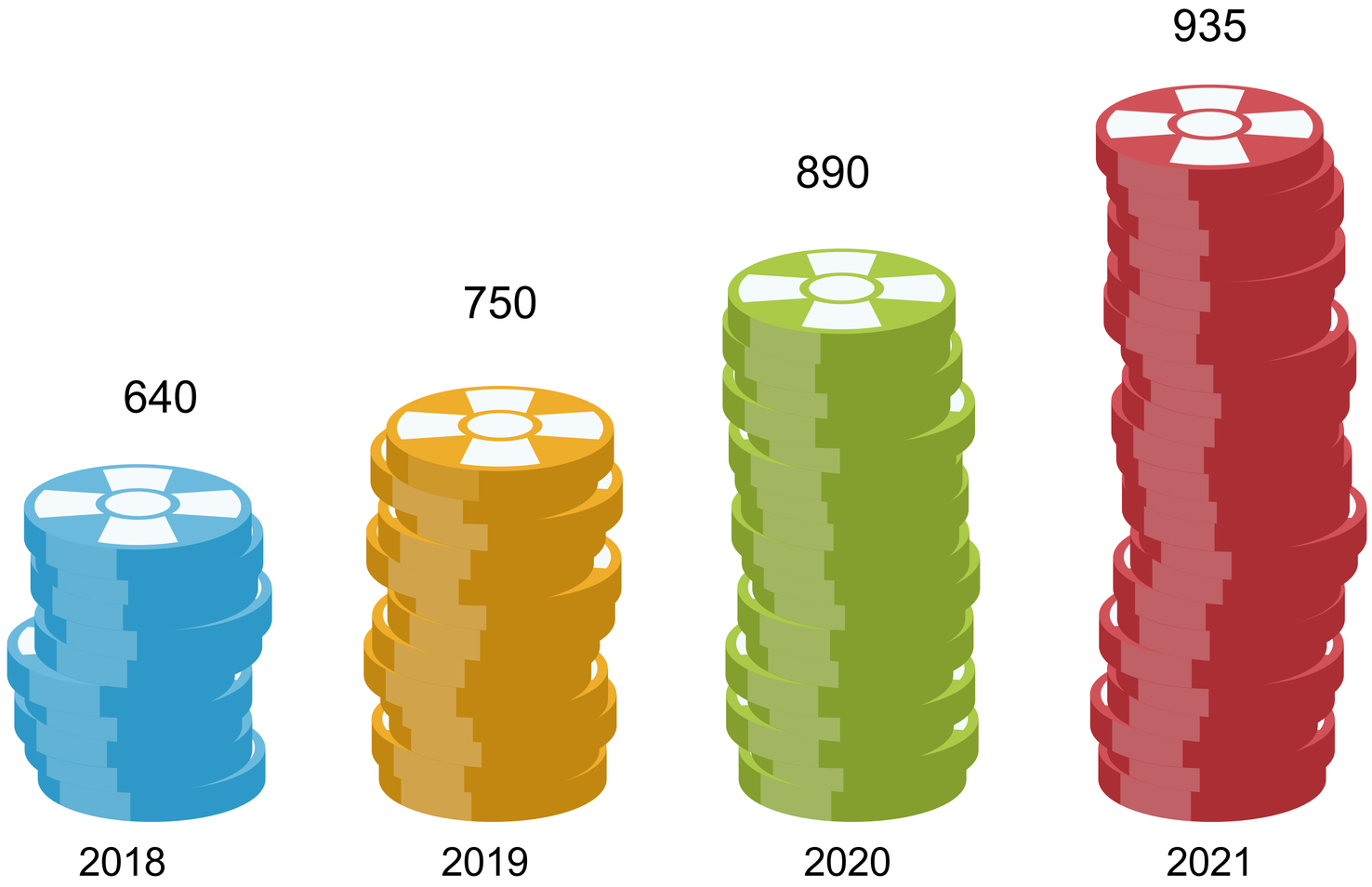
Cechy szczególne przestępstw cybernetycznych

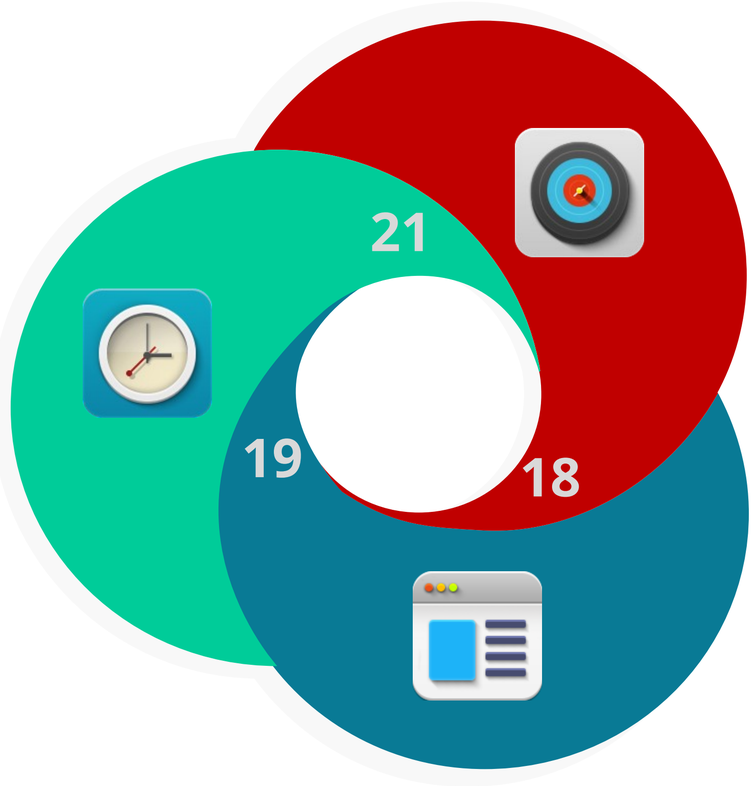
- Zwiększona skrytość popełnienia przestępstwa – w zasadzie przestępca może być niewidoczny;
- Transgraniczny charakter przestępstw w sieciach, w których sprawca, przedmiot przestępstwa oraz jego ofiara mogą znajdować się na terytoriach różnych państw, nierzadko poza jurysdykcją ojczyzny ofiary;
- Specjalistyczne przygotowanie przestępców, intelektualny charakter działalności przestępczej;
- Możliwość automatyzacji prowadzenia działalności przestępczej, która może być wykonywana z wielu miejsc jednocześnie;
- Brak świadomości pokrzywdzonych, że byli narażeni na przestępstwo;
- Zdalny charakter działań przestępczych w warunkach braku kontaktu fizycznego sprawcy i pokrzywdzonego, może dzielić ich tysiące kilometrów;
- Niemożność zapobiegania i ograniczania przestępstw tego typu za pomocą tradycyjnych środków – słaby poziom przygotowania zawodowego formacji zaangażowanych w zwalczanie tego typu przestępstw.



Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Koszty cyberprzestępczości w mld USD

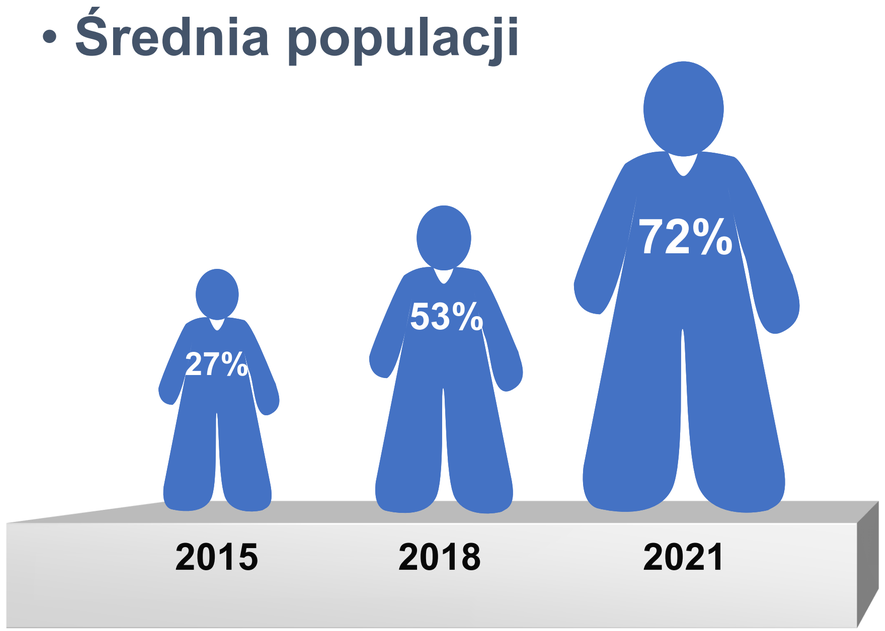




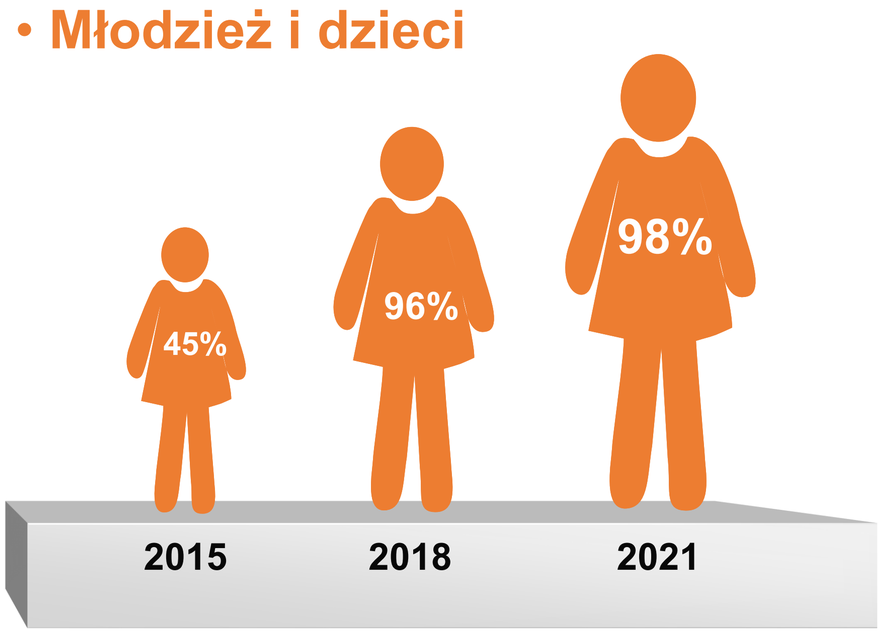
Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Poziom styczności z cybeprzestępczością w Polsce

Dzieci i młodzież są szczególnie narażone na skutki cyberprzestępczości, o czym świadczą dane statystyczne. Ofiarami mogą być również osoby starsze, coraz częściej korzystające z technik komputerowych.



Osoby mające kontakt z cyberprzestępczością, w %

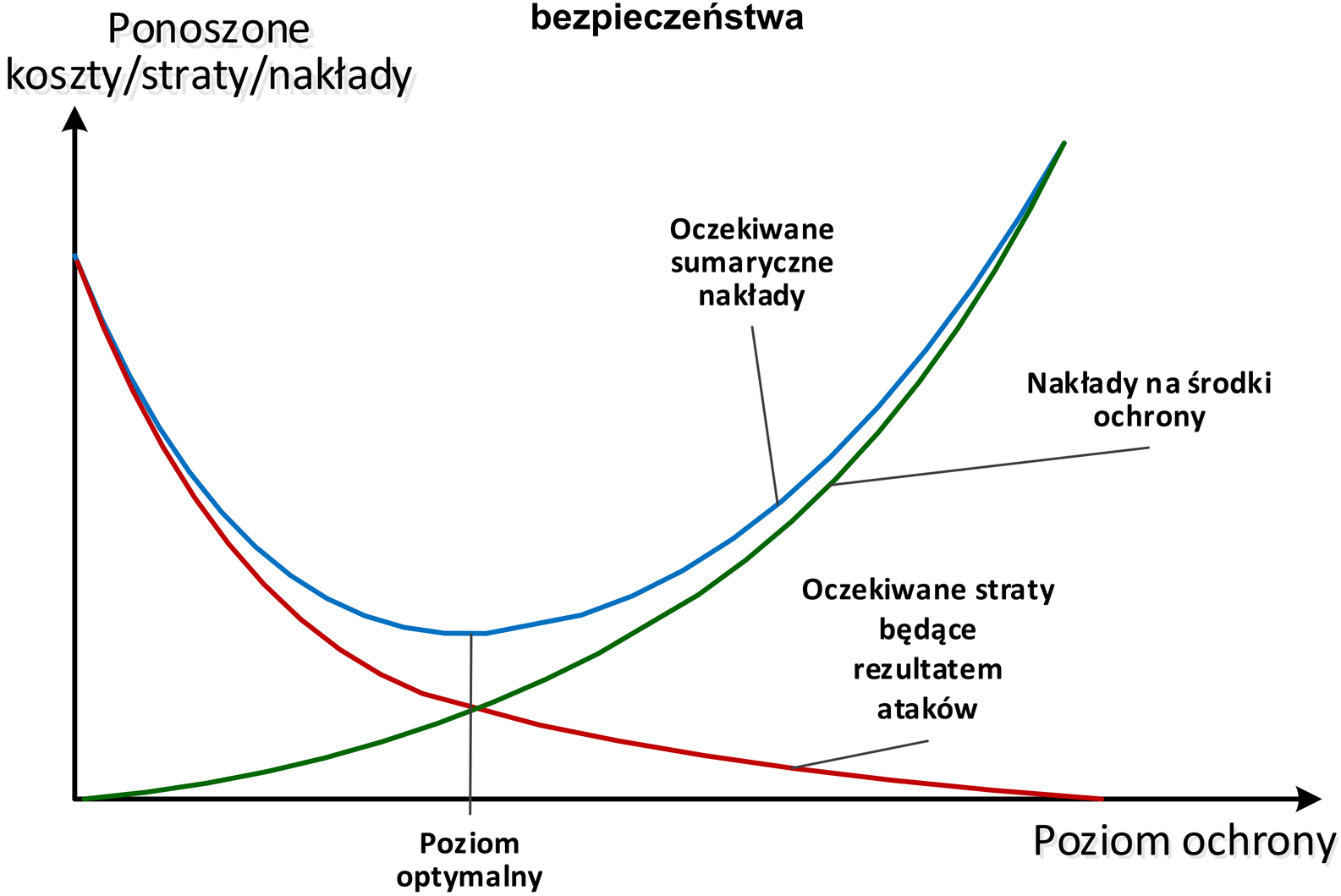


Młodzież mająca dostęp z cyberprzestępczością, w %

Polacy są bardzo szybko starzejącym się społeczeństwem. Na szczęście, osoby starsze są coraz lepiej wyedukowane i względnie dobrze sobie radzą z wykorzystaniem nowoczesnych technik informacyjnych. Najlepiej wyedukowanym informatycznie społeczeństwem (bez względu na wiek) są Amerykanie.

Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Podstawowe ograniczenia ochrony bezpieczeństwa



Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Komponenty bezpieczeństwa informacji

Bezpieczeństwo informacji
Ochrona informacji chronionej i przetwarzanej w systemie przed zagrożeniami wewnętrznymi i zewnętrznymi

01

Bezpieczeństwo infrastruktury
Ochrona programowych i sprzętowych elementów systemu przed zagrożeniami wewnętrznymi i zewnętrznymi

02

Bezpieczeństwo zewnętrzne
Ochrona środowiska zewnętrznego przed zagrożeniami informacyjnymi z chronionego systemu

03

Zarządzanie bezpieczeństwem
Personel administrujący bezpieczeństwem powinien posiadać techniczne i organizacyjne możliwości zarządzania bezpieczeństwem

04

1973

1983

1990

1999

Kompletna ochrona bezpieczeństwa informacji musi uwzględniać wszelkie zagrożenia bezpieczeństwa systemu informacyjnego. Pierwotnie analizowano wyłącznie bezpieczeństwo informacji. Pojawienie się takich wirusów jak Stuxnet, Flame, Duqu, Gauss i in. ukierunkowanych na niszczenie infrastruktury sieciowej (przemysłowej), uświadomiło potrzebę ochrony infrastruktury. Żaden system informacyjny nie może zagrażać systemom zewnętrznym. Dlatego w systemach ochrony powinny znajdować się komponenty zapewniania bezpieczeństwa systemów zewnętrznych. Całość powinna być zarządzana.

Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Ogólna klasyfikacja działań cyberprzestępczych

Chociaż tradycyjne przestępstwa nadal stanowią utrapienie społeczeństwa, do asortymentu zagrożeń dołączyły przestępstwa o charakterze cybernetycznym. Większość cyberataków jest przeprowadzana przez cyberprzestępców lub hakerów w celu osiągnięcia zysku finansowego. Jednak celem cyberataków może być wyłączenie komputerów lub sieci, mogą być one prowadzone z motywów osobistych lub politycznych.
Cyberprzestępstwa są popełniane przez osoby i organizacje - od początkujących hakerów po dobrze skoordynowane grupy, które stosują zaawansowane techniki i są dobrze obeznane z technologią.

Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Ogólna klasyfikacja działań cyberprzestępczych

Jak zmieniały się motywy działania hackerów w przeciągu ostatnich trzech dekad? Zmiany można podsumować jednym zdaniem: *coraz mniej ideowości, coraz więcej komercji i ideologii*. Niestety z etosu hackerów lat 90-tych niewiele już pozostało. Obecnie hackerstwo to najzwyklejszy zawód lub nie zawsze legalna działalność polityczna. Popularność motywów nie przekłada się na liczbę skutecznych ataków. Hackerów zatrudniają również rządy państw, większość liczących się krajów posiada wojska cyberbetyczne, których zadaniem jest obrona przed atakami , a czasami realizacja takich.

Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

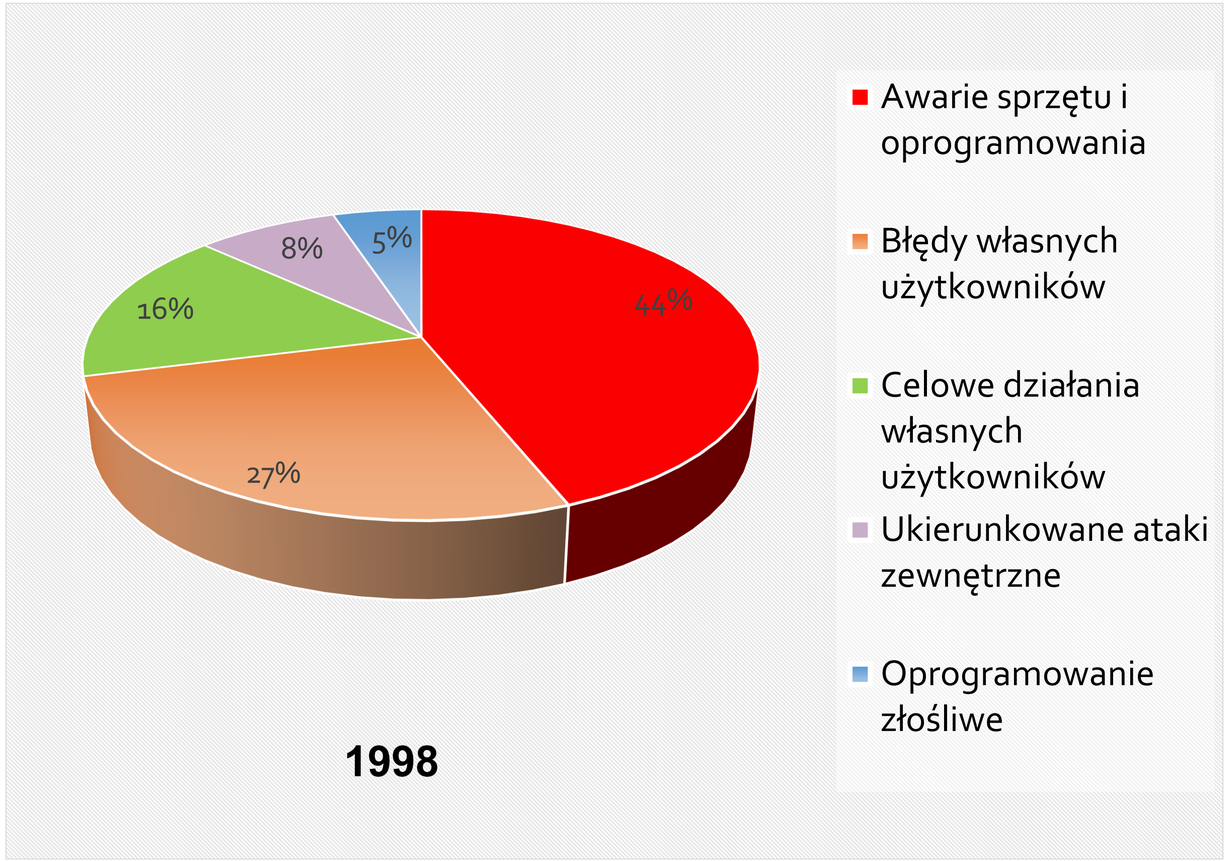
Haktywizm

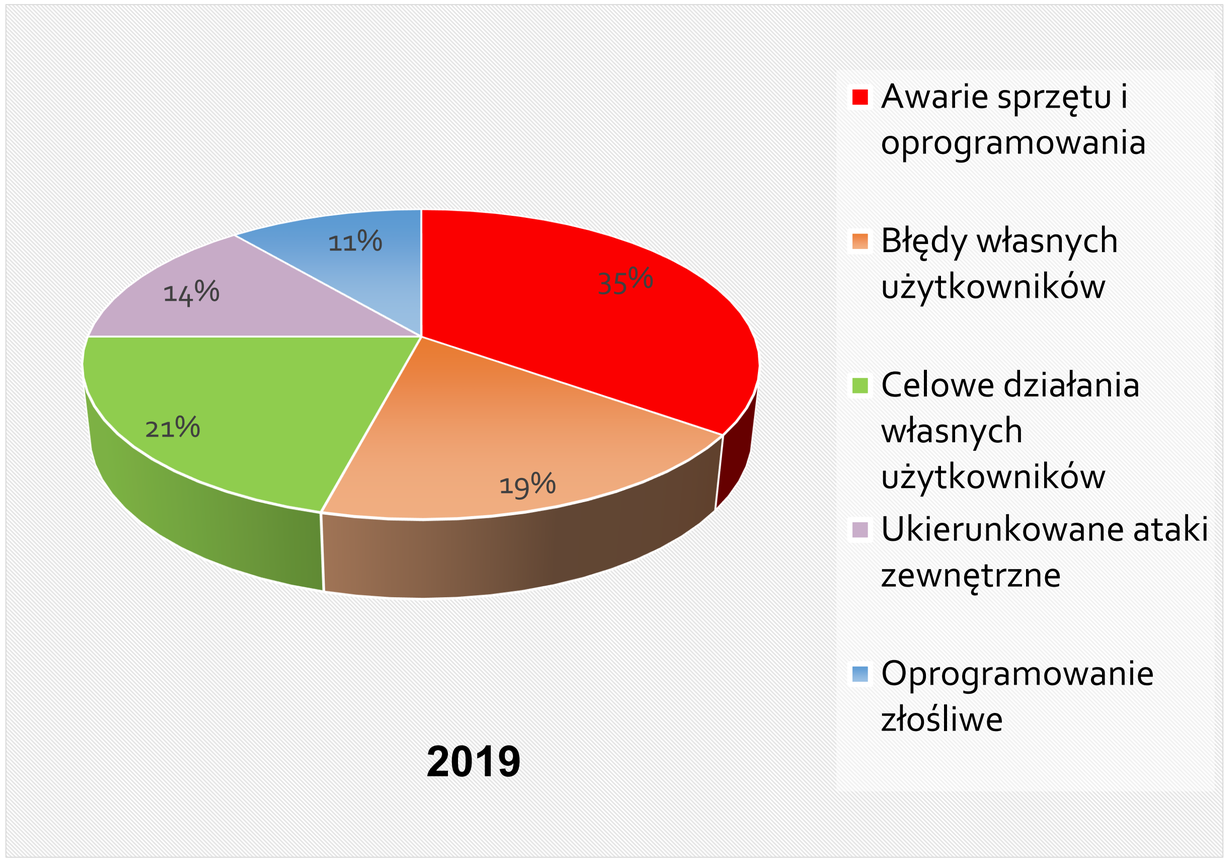
Działania znajdujące się na granicy cyberprzestępczości są szeroko wykorzystywane przez reżimy autorytarne do szerzenia dezinformacji, kształtowania opinii publicznej, fałszowania wyborów. W krajach demokratycznych niezbędne staje się wspomaganie rozróżniania informacji fałszywych od prawdziwych, coraz częściej wykonywane metodami maszynowymi bazującymi na sztucznej inteligencji. Nieoceniona jest również rola wolnych mediów.

Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Podstawowe zagrożenia bezpieczeństwa informacyjnego

Początkowo, systemy informacyjne rzadko były celem ataków hackerskich. Wynikało to z ich odseparowania od sieci - włamywacz nie posiadał bezpiecznego dostępu do ich zasobów. Sytuacja zmieniła się w momencie masowości usług internetowych i samego dostępu sieci. Z czasem jakość sprzętu i oprogramowania poprawiała się, a w sieci Internet pojawiały się coraz to nowe zasoby. Wtedy ataki na zasoby systemów stały się sposobem na zarobkowanie. Celowe ataki za którymi stoi osoba stanowią obecnie czwartą część wszystkich ataków na systemy informacyjne.

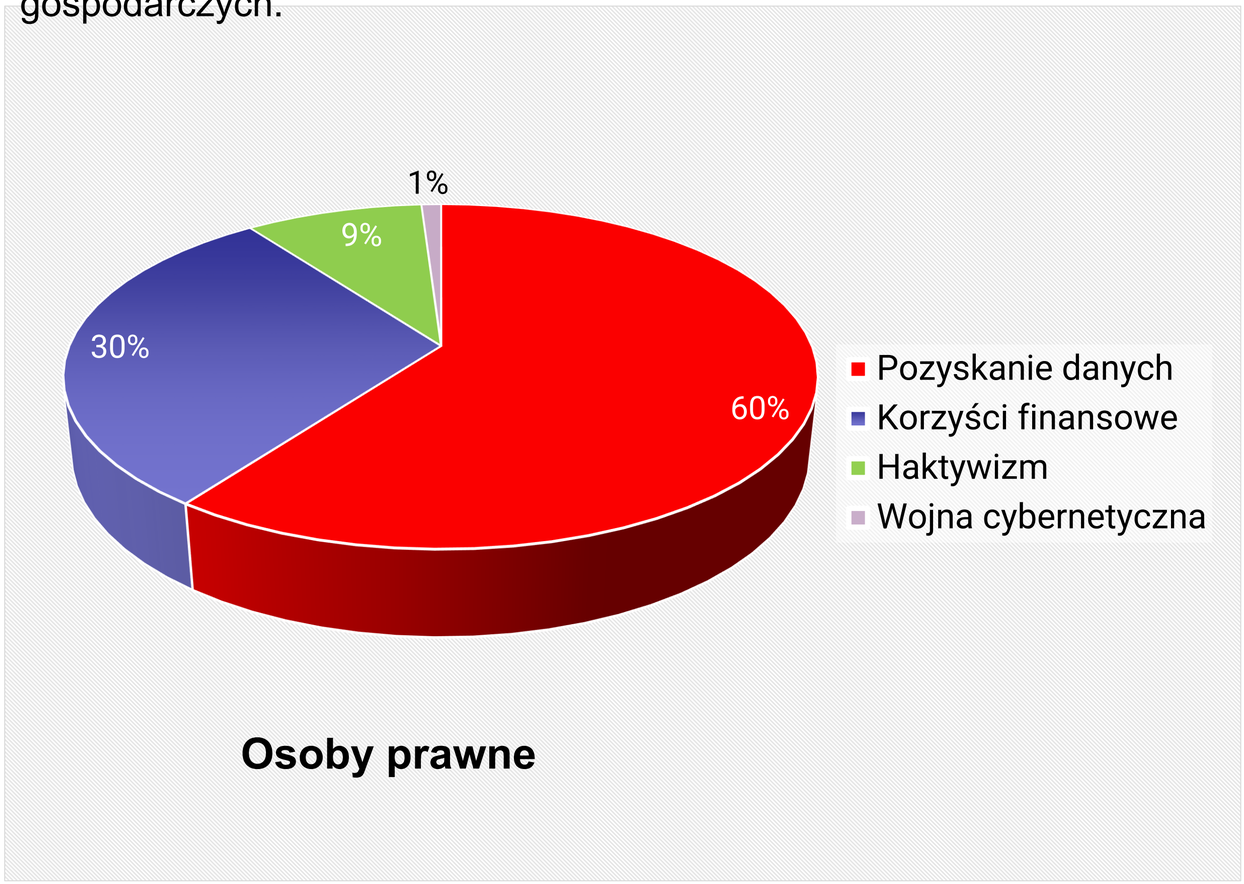




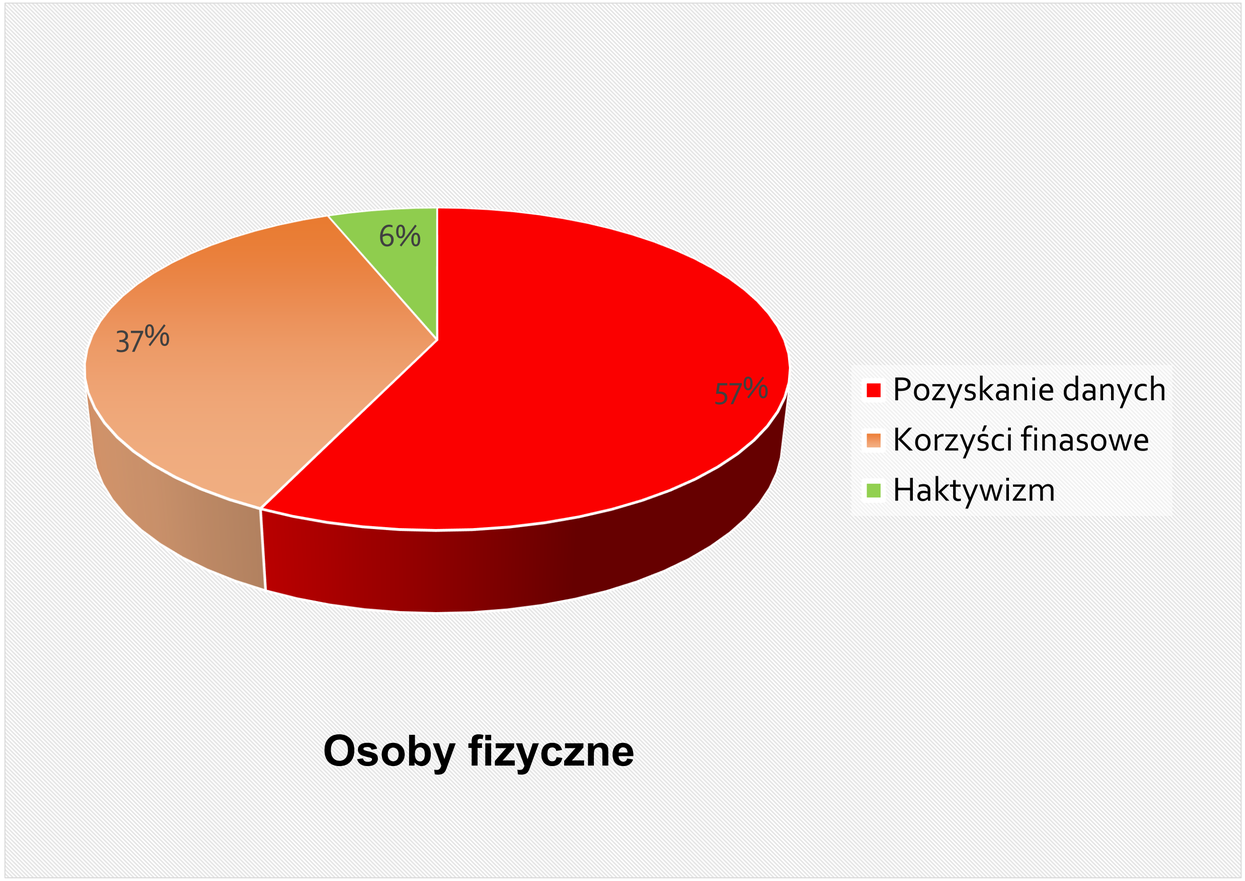
Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Cele działania hackerów w 2019 roku

Jeżeli w podmiocie gospodarczym, edukacji lub administracji przetwarzane są dane ich obsługa jest obwarowana szeregiem przepisów zapewniających bezpieczeństwo. Chociaż trudno jest mówić o ich bezpieczeństwie ich pozyskanie staje się coraz trudniejsze. Sprzyja temu również poprawa jakości wykorzystywanego oprogramowania. Dlatego systemy informacyjne osób prywatnych atakowane są częściej niż podmiotów gospodarczych.



Osoby prawne

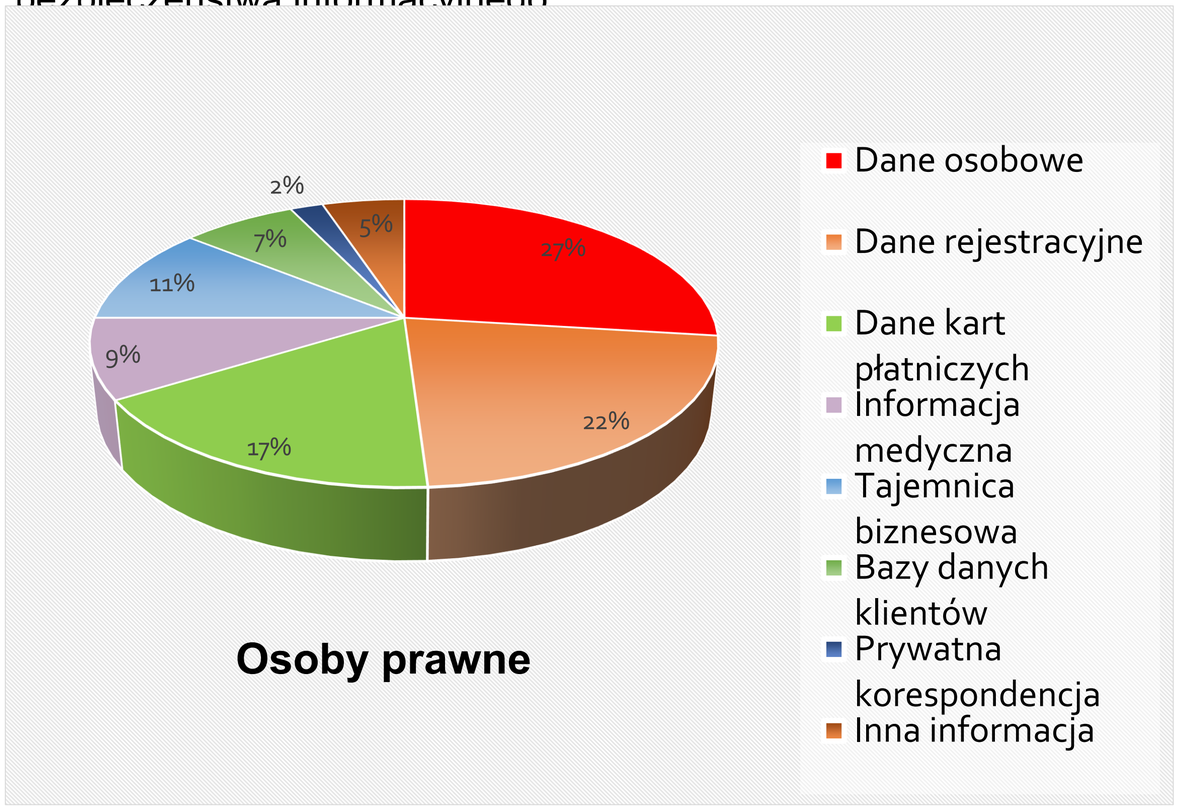


Osoby fizyczne

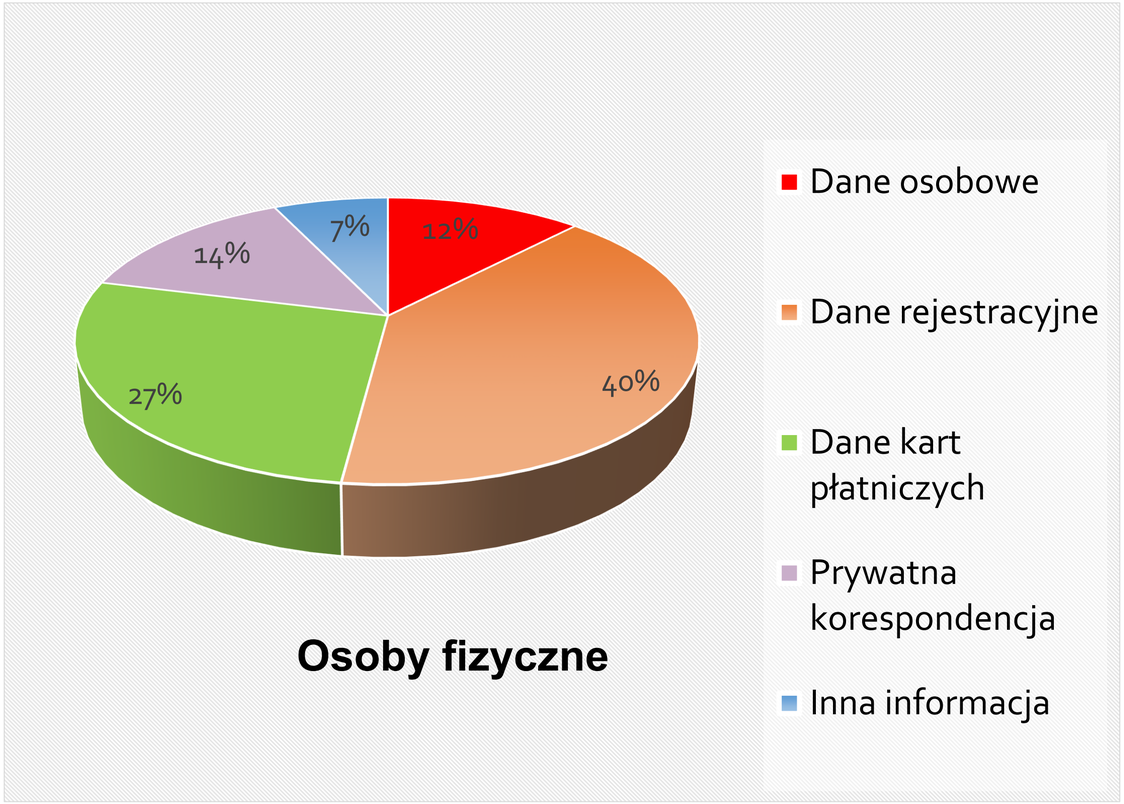
Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Typy pozyskiwanych danych w 2019 roku

Hackerzy pozyskują głównie te typy informacji, które posiadają wartość komercyjną. Informacje te są najczęściej odsprzedawane zainteresowanym podmiotom lub osobom. Dla osób prawnych największym zainteresowaniem cieszą się dane osobowe (chronione rozporządzeniem RODO) oraz dane pozwalające uzyskać dostęp do kont użytkowników (dane rejestracyjne). Obecnie osoby fizyczne to dla hackerów źródło łatwego zarobkowania (przynajmniej teoretycznie). Dlatego w pierwszej kolejności atakowane są ich dane rejestracyjne oraz dane kart płatniczych. Ich dane osobowe są zdecydowanie mniej interesujące. W związku z powyższym konieczne jest ciągłe kształcenie użytkowników prywatnych w obszarze bezpieczeństwa informacyjnego.



Osoby prawne



Osoby fizyczne

Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Najdotkliwsze zagrożenia bezpieczeństwa w 2022

Obszar obejmowany przez cyberprzestępczość zmienia się wraz z postępem technologicznym. Atakowane są głównie nowe obszary, w których zabezpieczenia nie są jeszcze doskonałe a sam atak pozawala osiągnąć założone cele.

- **Ataki na infrastrukturę krytyczną**

  Włamania do systemów obsługujących infrastrukturę krytyczną celem jej unieruchomienia.

- **Ataki na Internet rzeczy**

  Ataki na inteligentny sprzęt pomiarowy Smart City celem pozyskania informacji lub dezinformacji.

- **Ataki na prywatność**

  Ataki na m.in. kamery internetowe, szczególnie umieszczane w domach prywatnych lub infrastrukturze Smart City, odszywanie się pod użytkowników.

- **Ataki na sprzęt mobilny**

  Ataki na operacje wykonywane za pomocą urządzeń przenośnych, w szczególności smartfonów, ataki na mobile sensory pomiarowe Smart City.

Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Czym przestępcy zagrażają użytkownikom sieci

Dzieci ofiarami cyberprzestępstwa

Ofiarami cyberprzestępstw są najczęściej osoby nieletnie. Najtragiczniejszym i nieodwracalnym przykładem cyberterroryzmu ukierunkowanego na dzieci jest masowe angażowanie ich w grupy samobójcze, w których promowana jest śmierć jako sposób ucieczki od życia.
Przestępcy wykorzystują różne metody wpływania na dzieci: od bezpośredniej korespondencji w sieciach społecznościowych, po wspólne oglądanie filmów, dyskusje na temat seriali telewizyjnych, pomoc w rozwiązywaniu zadań domowych, dostęp do książek online, pomoc w doborze literatury beletrystycznej, wspólne słuchanie muzyki.

Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Ewolucja systemów informacyjnych a koncepcja Smart City

przed 1945

Programowane architektury

Określono zasady prowadzenia prac badawczych, oddelegowano osoby do pracy w *Projekcie* ze wskazaniem ich zadań, określono zasady wynagradzania pracowników.

1945

Komputery programowane

Prace badawcze zostały podzielona na grupy tematyczne ze zdefiniowanym obszarem. Do każdej z grup przydzielony został zespół badawczy, najczęściej 1-2 osoby.

1964

Komputery mainframe

Dokonano przeglądu źródeł w zdefiniowanych wcześnie grupach tematycznych. Na ich podstawie uszczegółowiono zadania badawcze.

1981

Komputery personalne

Scentralizowane dotąd gromadzenie i przetwarzanie danych zostało rozproszone za pomocą prostych architektonicznie i łatwych w eksploatacji komputerów personalnych

Istotą systemów Smart City jest rozproszenie procesu pozyskiwania danych

1991

Sieci komputerowe

W celu zapewnienia spójności informacyjnej o umożliwienia skalowalności komputery personalne połączono za pomocą sieci komputerowych

Sieci komputerowe stały się bazą do rozwoju komunikacji komponentów Smart City

2010

Internet rzeczy

Rozproszenie gromadzenia i przetwarzania danych. Zastosowanie inteligentnych sensorów pomiarowych, chmur danych i obliczeń, ros i mgieł obliczeniowych, systemów obliczeń brzegowych

Dopiero Internet rzeczy zapewnił możliwość nieskrępowanego rozwoju Smart City

Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Klasyfikacja zagrożeń systemów Smart City

Zagrożenie 1

Końcowym odbiorcą informacji pochodzącej z Smart City jest również człowiek

Zagrożenie 2

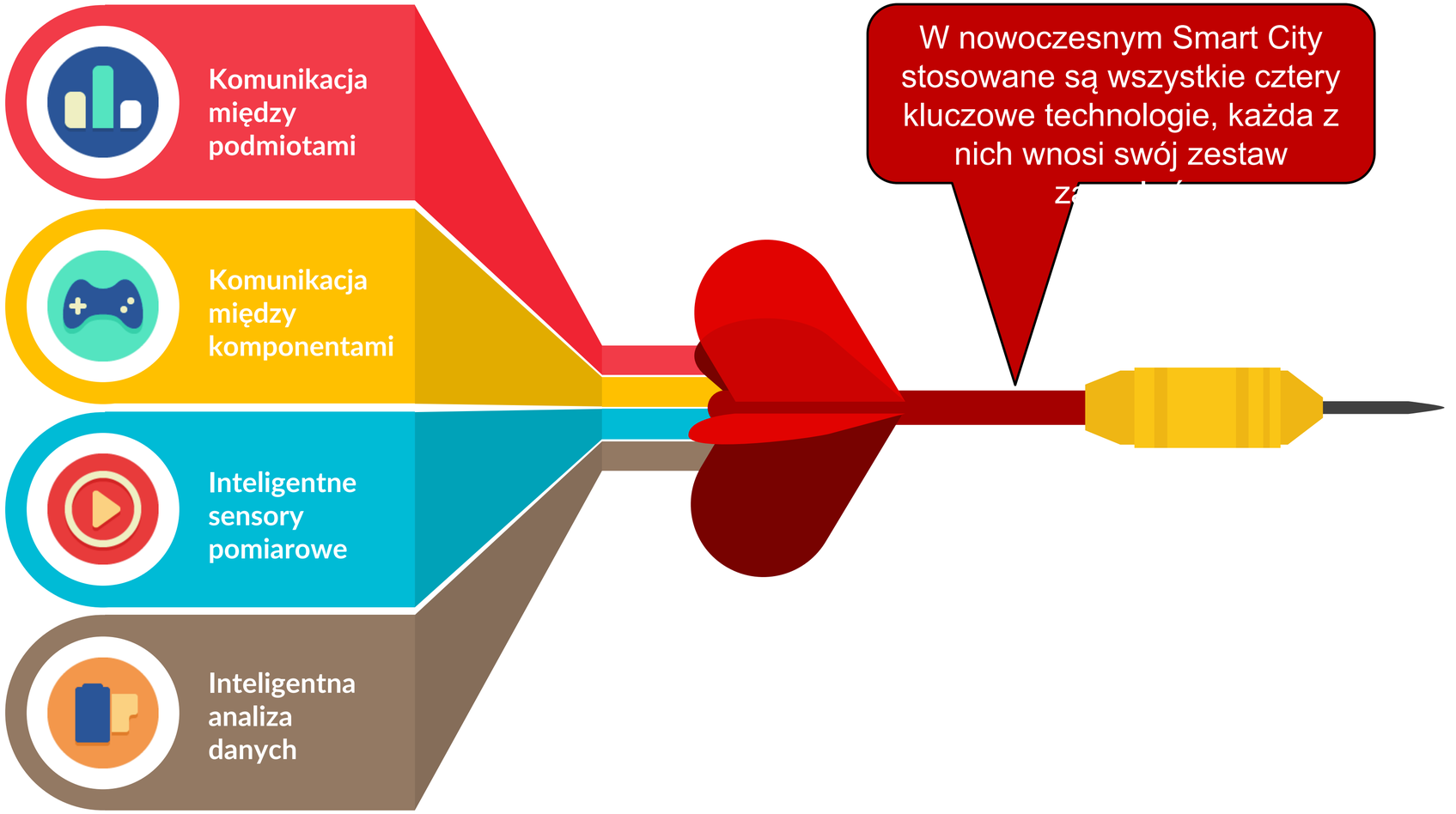
Komunikacja pomiędzy komponentami Platformy Smart City może być sabotowana

Zagrożenie 3

Pomiary wykonywane w technologii IoT, oferowane są możliwości obliczeń brzegowych

Zagrożenie 4

Analiza danych pomiarowych szeroko stosuje metody sztucznej inteligencji



Zagrożenie 5

Efekt synergii może powodować zarówno wzrost jak i ograniczenie zagrożeń bezpieczeństwa

Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Zagrożenia systemów Smart City

Komunikacja między podmiotami

Szeroko wykorzystuje metody i środki komunikacji człowiek-maszyna. Eliminuje błędy w rozumieniu prezentowanej informacji, np. przez seniorów. Możliwe ataki socjotechniczne i dezinformacja.

Komunikacja między komponentami

Zapewnia spójność informacyjną systemu oraz sterowanie elementów wykonawczych. Atrakcyjny obiekt ataku.

Inteligentne sensory pomiarowe

Dokonują pomiaru i wstępnego przetworzenia (analizy) danych. Oferują obliczenia brzegowe. Atrakcyjny obiekt ataku.

Inteligentna analiza danych

Wykorzystywana do prognozowania z najwyższym prawdopodobieństwem zachowań systemu i doboru działań zaradczych. Wykonywana centralnie.

Architektura Smart City

Połączenie wszystkich zastosowanych technologii zazwyczaj powoduje poprawę poziomu cyberbezpieczeństwa

Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Ataki na systemy Smart City oparte na IoT

Podsłuchiwanie połączeń

- **Istota ataku:** Podsłuchiwanie to atak, który pozwala atakującemu wydobyć poufne i szybkie informacje, które można wykorzystać do złośliwych działań, w tym kolejnych ataków na systemy IoT. Często podsłuchiwanie i zbieranie informacji są początkowym etapem cyberataków, z ich pomocą identyfikowane są słabe punkty i potencjalne punkty wejścia ataku;
- **Skutki:** głównym rezultatem jest naruszenie poufności danych. W zależności od środowiska stopień zagrożenia może być różny – wyższy lub niższy. Podsłuchiwanie może sygnalizować nadchodzący atak na większą skalę.
- **Powiązane zagrożenia:** podsłuchiwanie i wyciek poufnych danych.
- **Stopień zagrożenia atakiem:** wysoki - krytyczny.

Atak na sensory pomiarowe

- **Istota ataku:** Sprowadza się do zaatakowania czujników pomiarowych i zmiany odczytywanych przez nie wartości lub ich progów oraz innych ustawień. Atakujący manipuluje konfiguracją czujników, zmieniając ustawione na nich progi, aby umożliwić akceptowanie przez nie wartości poza dopuszczalnym zakresem, co stanowi poważne zagrożenie dla systemu i jego urządzeń. Ponieważ większe urządzenia zwykle używają wielu zduplikowanych czujników, aby atak był skuteczny, atakujący musiałby narazić na szwank wiele czujników, w przeciwnym przypadku atak byłby zidentyfikowany.
- **Skutki:** Zezwolenie czujnikowi na akceptację nieprawidłowych wartości naraża środowisko IoT na uszkodzenie, np. przez skok napięcia przeoczony przez uszkodzony sensor;
- **Powiązane zagrożenia:**. atak na prywatność, wyciek poufnych danych, zamiana informacji.
- **Stopień zagrożenia atakiem:** wysoki - krytyczny.

Ataki na elementy wykonawcze

- **Istota ataku:** Atak sprowadza się do zmiany lub sabotowania ustawień urządzeń wykonawczych. Przykładem jest manipulowanie konfiguracją lub parametrami siłowników, powodujące stosowanie przez nie niewłaściwych konfiguracji, progów lub danych, co wpływa na ich normalne zachowanie, zakłócając ich właściwe ustawienia operacyjne.
- **Skutki:** Jest różny w zależności od celu ataków. Może mieć wpływ na procesy produkcyjne.
- **Powiązane zagrożenia:** Awarie sieci i naruszenia bezpieczeństwa przez złośliwe (zainfekowane) urządzenia.
- **Stopień zagrożenia atakiem:** wysoki - krytyczny.

Atak na systemy zarządzania IIoT

- **Istota ataku:** Osoba atakująca próbuje uzyskać pełną kontrolę nad systemem administracyjnym systemu IoT lub urządzenia IoT, co może zagrozić całemu środowisku. Wdrożenie takiego ataku nie jest trudne, jeśli używane są słabe hasła lub hasła domyślne. Ten rodzaj ataku składa się z kilku etapów i jest zwykle przeprowadzany w ukryciu. Należy zauważyć, że na pojawienie się tego typu ataków trzeba być przygotowanym przez cały cykl życia urządzenia lub systemu;
- **Skutki:** naruszenie bezpieczeństwa, manipulacja lub przerwanie działania niektórych systemów IoT może mieć wpływ na wiele osób, spowodować problemy środowiskowe, a nawet rozprzestrzenić się na inne systemy, wpływając na ich komunikację lub nawet je zamykając;
- **Powiązane zagrożenia:**. słabe hasła, zestawy exploitów, ataki na prywatność, złośliwe oprogramowanie i ataki DDoS.
- **Stopień zagrożenia atakiem:** wysoki - krytyczny.

Cyberbezpieczeństwo w rozwoju i upowszechnianiu koncepcji Smart City

Ataki na systemy Smart City oparte na IoT

Luki w protokołach

- **Istota ataku:** Ten typ jest zwykle pośrednikiem podczas przeprowadzania innych rodzajów ataków. Exploity (luki w zabezpieczeniach) są wykorzystywane w celu uzyskania uprzywilejowanego nieautoryzowanego dostępu do systemu, co może skutkować instalacją innych złośliwych treści lub backdoorów. Są one wykorzystywane jako część ataku, niezależnie od tego, czy celem jest pojedynczy system, urządzenie czy cała sieć. Wykrywanie exploitów jest trudne, łatwiej jest wykryć działania wykonane po skutecznym wdrożeniu exploita.;
- **Skutki:** jeśli atak się powiedzie, exploit tworzy punkt wejścia, w niektórych przypadkach z podwyższonymi uprawnieniami, w przeciwnym razie system może ulec awarii lub stać się niestabilny. Ten atak jest zawsze używany jako część większego ataku, który może być zwykłą kradzieżą danych;
- **Powiązane zagrożenia:** zestawy exploitów, złośliwe oprogramowanie;
- **Stopień zagrożenia atakiem:** wysoki .

Wprowadzenie polecenia na konsolę

- **Istota ataku:** W tego typu ataku osoba atakująca za pośrednictwem swojej konsoli wprowadza i wykonuje polecenia z uprawnieniami administratora w zaatakowanym systemie.
- **Skutki:** Jeśli osoba atakująca może wprowadzić polecenia do urządzenia, istnieje możliwość włamania się do innego urządzenia maszyny w otoczeniu. Spowoduje to efekt kaskadowy w systemie, a osoba atakująca będzie mogła wykorzystać wszystkie te urządzenia do wrogich celów;
- **Powiązane zagrożenia:**. Zestawy eksploitów, ataki typu DDoS;
- **Stopień zagrożenia atakiem:** wysoki - krytyczny.

Ataki krokowe

- **Istota ataku:** Ten rodzaj ataku jest powszechnym sposobem przeprowadzania anonimowych ataków. Ataki te są często wykorzystywane przez atakujących w sieci, aby ukryć swoją tożsamość, ponieważ przeprowadzają ataki nie ze swojego komputera, ale z hostów pośrednich, które wcześniej skompromitowali;
- **Skutki:** Jeśli atakujący przeprowadzi atak krokowy, może narazić na szwank zbiór węzłów sieci, wykorzystując je jako odskocznie do przekazywania dalej poleceń ataku..
- **Powiązane zagrożenia:** Ataki DDoS, fałszowanie złośliwych urządzeń.
- **Stopień zagrożenia atakiem:** średni - wysoki.

Atak na źródła zasilania

- **Istota ataku:** Mają na celu manipulowanie zasilaczami i wykorzystywanie luk w ich zabezpieczeniach w celu zmiany odczytywanych danych o zasilaniu. Atakujący może fizycznie uszkodzić baterię urządzenia lub kable zasilające lub manipulując źródłem zasilania poprzez złośliwe oprogramowanie. Można zmieniać sposoby odczytu informacji o poziomie naładowania, aby spowodować, że urządzenie uzna, że poziom naładowania baterii jest wyższy lub niższy niż rzeczywisty;
- **Skutki:** fizyczna ingerencja w baterię może ją uszkodzić i urządzenie nie będzie działać. Manipulowanie sposobem, w jaki urządzenie odczytuje poziom naładowania akumulatora, może spowodować, że urządzenie uzna, że poziom naładowania akumulatora jest wyższy lub niższy niż rzeczywisty, co wpływając na żywotność urządzenia;
- **Powiązane zagrożenia:**. programy złośliwe, ataki fizyczne;
- **Stopień zagrożenia atakiem:** średni - wysoki.


THE