Jakość i rzetelność aplikacji mobilnych z perspektywy developera

carnalife medapp

Mateusz Kierepka
CEO

MedTrends

Prawo i zalecenia

Podstawy prawne i organizacyjne

•Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2016 r. poz. 1535),
•Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2014 r. poz. 1114, z późn. zm.),
•Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. z 2016 r. poz. 1793, z późn. zm.),
•Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz.U. z 2016 r. poz. 1868, z późn. zm.),
•Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U. z 2016 r. poz. 1638 i 2260),
•Ustawa z dnia 6 września 2001 r. prawo farmaceutyczne (Dz.U. z 2016 r. poz. 2142),
•Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2016 r. poz. 186, z późn. zm.),
•Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz.U. 2017 poz. 125),
•Ustawa z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz.U. 2016 poz. 1866),
•Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2016 r. poz. 922),
•Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2016 r. poz. 1167),
•Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579),
•Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2015 poz. 2069),
•Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz.U. 2015 r. poz. 971),
•Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2016 r. poz. 113),
•Rozporządzenie Ministra Zdrowia z dnia 25 marca 2013 r. w sprawie klasyfikacji danych i systemu kodów w Systemie Informacji Medycznej (Dz.U. 2013 r. poz. 473 z późn. zm.),
•Rozporządzenie Ministra Zdrowia z dnia 28 marca 2013 r. w sprawie wymagań dla Systemu Informacji Medycznej (Dz.U. 2013 r. poz. 463 z późn. zm.),
•Rozporządzenie Ministra Sprawiedliwości z dnia 26 lutego 2016 r. w sprawie rodzajów i zakresu dokumentacji medycznej prowadzonej w podmiotach leczniczych dla osób pozbawionych wolności oraz sposobu jej przetwarzania (Dz.U. 2016 poz. 258),
•Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 2004 r. Nr 100 poz. 1024),

Podstawy prawne i organizacyjne

•Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz.U. 2006 r. Nr 206 poz. 1518),
•Rozporządzenie Ministra Cy999fryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (Dz.U. 2016 poz. 1626),
•Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 25 lutego 2016 r. w sprawie rodzajów, zakresu i wzorów oraz sposobu przetwarzania dokumentacji medycznej w podmiotach leczniczych utworzonych przez ministra właściwego do spraw wewnętrznych (Dz.U. 2016 poz. 249),
•Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW,
•Rozporządzenie (UE) 2016/679 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylające dyrektywę 95/46/WE (ogólne rozporządzenie o ochronie danych),
•Dyrektywa Parlamentu Europejskiego i Rady (UE) w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii,
•Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE,
•Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
•Norma PN-EN 13609-1:2007 Informatyka w ochronie zdrowia -- Komunikaty do przechowywania informacji pomocniczych w systemach opieki zdrowotnej -- Część 1: Aktualizacja schematów kodowania,
•Norma PN-EN 13606-2:2009 Informatyka w ochronie zdrowia -- Przesyłanie elektronicznej dokumentacji zdrowotnej -- Część 2: Specyfikacja wymiany archetypów,
•Norma PN-EN 13606-3:2009 Informatyka w ochronie zdrowia -- Przesyłanie elektronicznej dokumentacji zdrowotnej -- Część 3: Archetypy referencyjne i listy terminów,
•Norma PN-EN 13606-4:2009 Informatyka w ochronie zdrowia - Przesyłanie elektronicznej dokumentacji zdrowotnej - Część 4: Bezpieczeństwo danych,

Podstawy prawne i organizacyjne

•Norma PN-EN ISO 13606-5:2010 - Informatyka w ochronie zdrowia -- Przesyłanie elektronicznej dokumentacji zdrowotnej -- Część 5: Specyfikacja interfejsu,
•Norma PN-ISO/IEC 27005:2014-01 Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji,
•ISO/IEC 27033-1 — IT network security – Overview and concepts,
•ISO/IEC 27033-1 — Information technology - Security techniques - Network security - Part 1: Overview and concepts,
•ISO/IEC 27033-2 — Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security,
•ISO/IEC 27033-3 — Information technology - Security techniques - Network security - Part 3: Reference networking scenarios -- Risks, design techniques and control issues,
•ISO/IEC 27033-4 — Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways - Risks, design techniques and control issues,
•ISO/IEC 27033-5 — Information technology - Security techniques - Network security - Part 5: Securing virtual private networks - Risks, design techniques and control issues,
•ISO/IEC 27033-6 — Information technology - Security techniques - Network security - Part 6: IP convergence,
•ISO/IEC 27033-7 — Information technology - Security techniques - Network security - Part 7: Wireless,
•PN-ISO/IEC 27001:2014-12 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania,
•PN-EN ISO 27799:2016-10 - Informatyka w ochronie zdrowia -- Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002,
•PN-ISO/IEC 27002:2014-12 Technika informatyczna -- Techniki bezpieczeństwa -- Praktyczne zasady zabezpieczania informacji,
•Norma PN-I-13335-1:1999 Technika informatyczna - Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych,
•Norma PN-I-13335-2:2003 Technika informatyczna – Planowanie i zarządzanie bezpieczeństwem systemów informatycznych,
•PN-EN ISO 10781:2015-11 Informatyka w ochronie zdrowia -- Model funkcjonalny systemu elektronicznej dokumentacji zdrowotnej HL7, wersja 2 (EHR FM),
•PN-EN ISO 21549-3:2014-05 - wersja angielska Informatyka w ochronie zdrowia -- Dane dotyczące karty zdrowia pacjenta -- Część 3: Ograniczony zestaw danych klinicznych.

Dostępne normy i standardy oraz polskie wytyczne

Rekomendacje: Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej (marzec 2017)
https://www.csioz.gov.pl/fileadmin/user_upload/rekomendacje_bezpieczenstwo_projekt_kwiecien2017_58f615848ab44.pdf
Opublikowany: 06.04.2017

MARS-E

The HIPAA Privacy Rule

The HIPAA Security Rule

The HITECH Breach Notification Final Rule

ISO/IEC 27018

ISO/IEC 27001

Title 21 CFR Part 11

Protection Directive 95/46/EC.

FedRAMP Moderate

FedRAMP High (Azure Government)

Organizacje specjalizujące się w cyberbezpieczeństwie (medycznym)

Wybrane artykuły organizacji:

- European Union Agency for Network and Information Security (ENISA)
  Security and Resilience in eHealth Security Challenges and Risks

Security and Resilience in eHealth Security Challenges and Risks

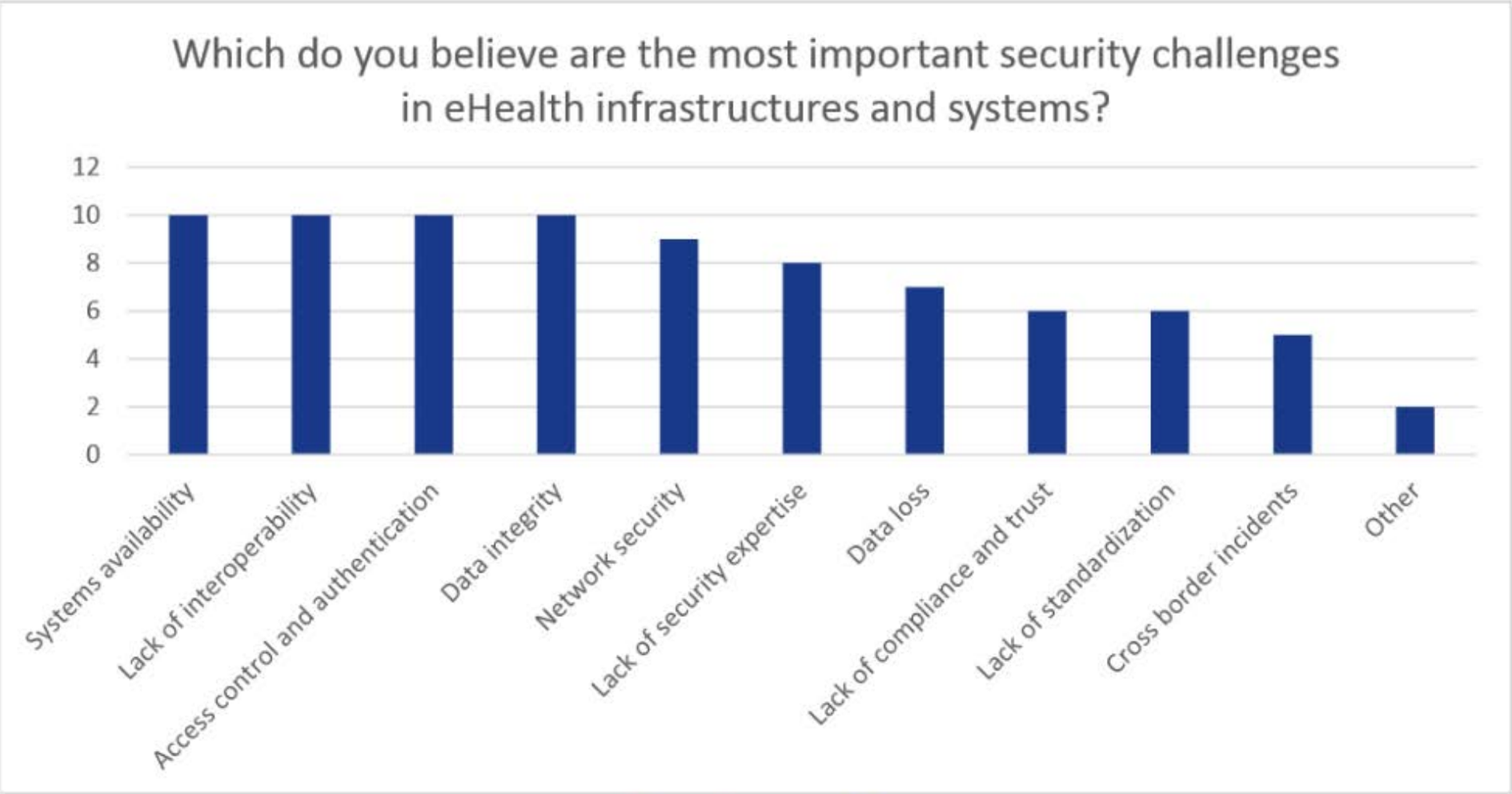


Figure 6 Security challenges

Security and Resilience in eHealth Security Challenges and Risks

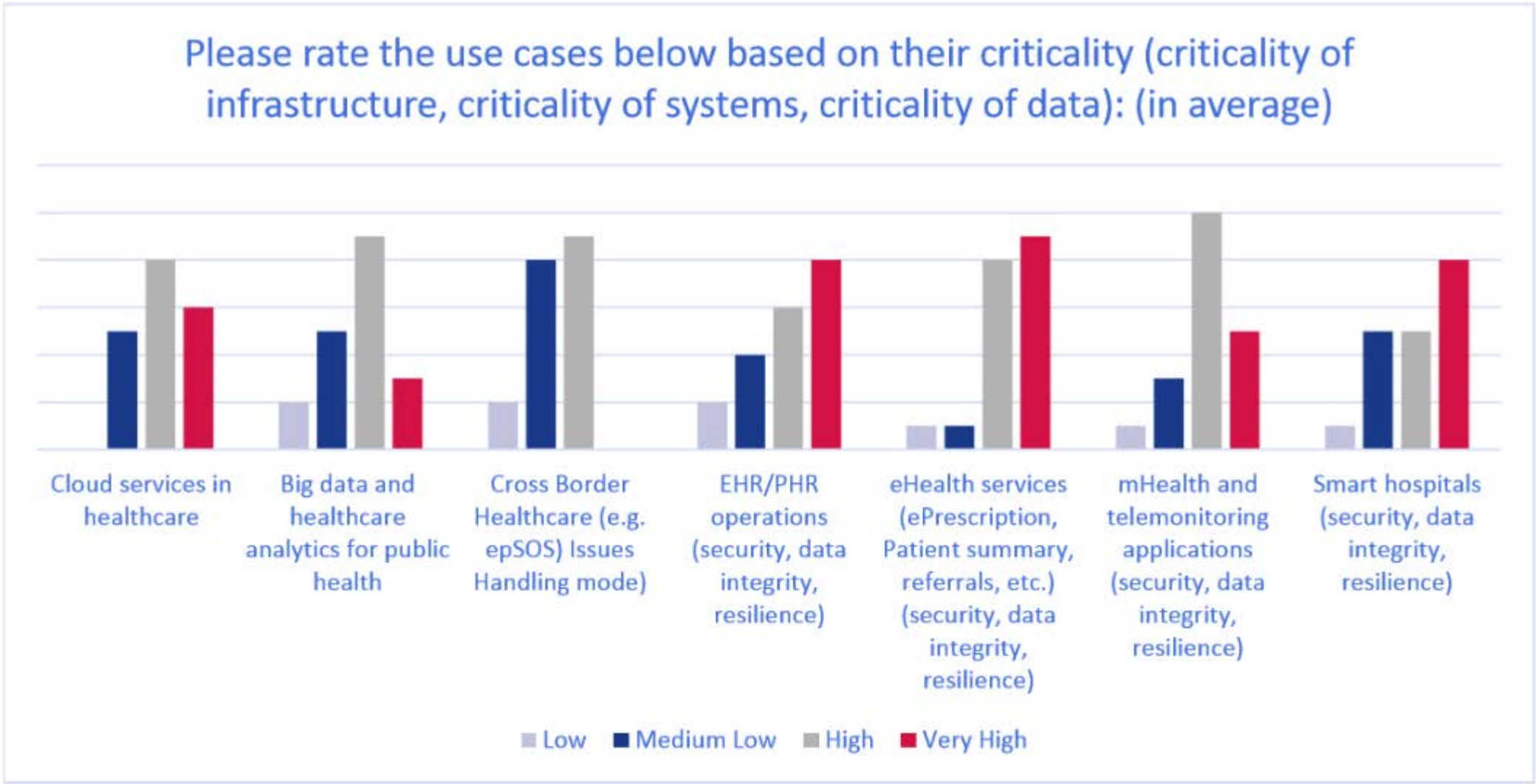
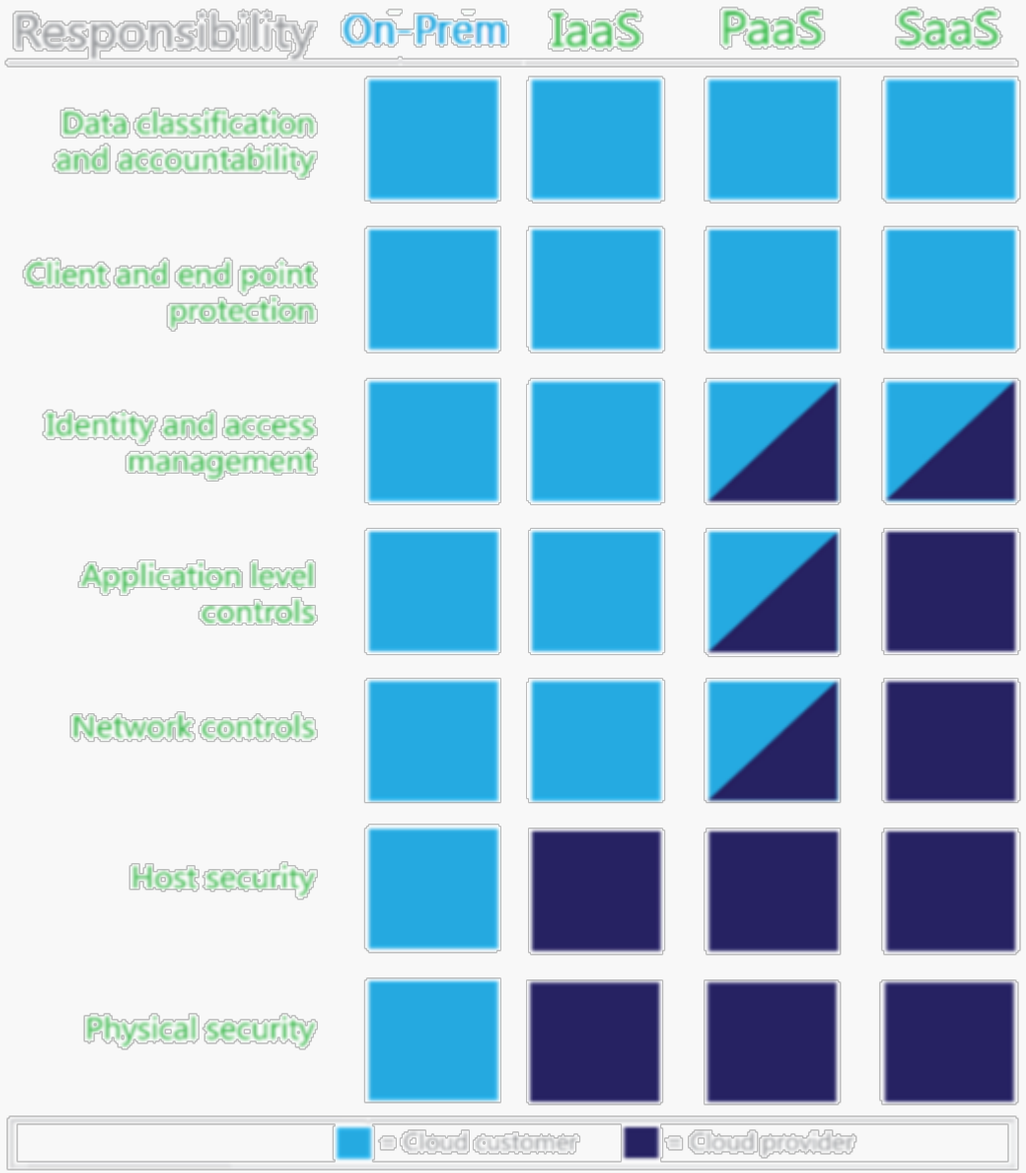


Figure 9–Criticality of Use cases

Rozwiązania chmurowe



Nadzór nad bezpieczeństwem chmury zapewniają różne organizacje jedną z nich jest:

cloud CSA security alliance®

https://microsoft.docs.contently.com/v/a-practical-guide-to-designing-secure-health-solutions-using-microsoft-azure?wt.mc_id=AID609949_QSG_BLOG_146742

Privacy Code of Conduct on mobile health apps

Komisja europejska wydała dokument roboczy dotyczący wytycznych i zasad tworzenia aplikacji mobilnych wykorzystywanych w zdrowiu. Główne wytyczne:

- Pewność przesyłania danych medycznych
- Limitacja wykorzystywania danych i minimalizacja zbierania danych
- Prywatność jako główne założenia
- Prawa pacjenta w dostępie do danych i informacji
- Przechowywanie danych – trwałość i okres ich przechowywania
- Zabezpieczenia i ich poziomy oraz sposoby pomiaru
- Reklamy i ich sposób użycia
- Sposób użycia danych osobistych
- Przesył danych w zależności od położenia w EU/EEA i prawa do wysyłania poza granice EU
- Sposoby zarządzania ryzykiem
- Pobieranie danych medycznych od dzieci

https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

General Data Protection Regulation 2016/679 ("**GDPR**")

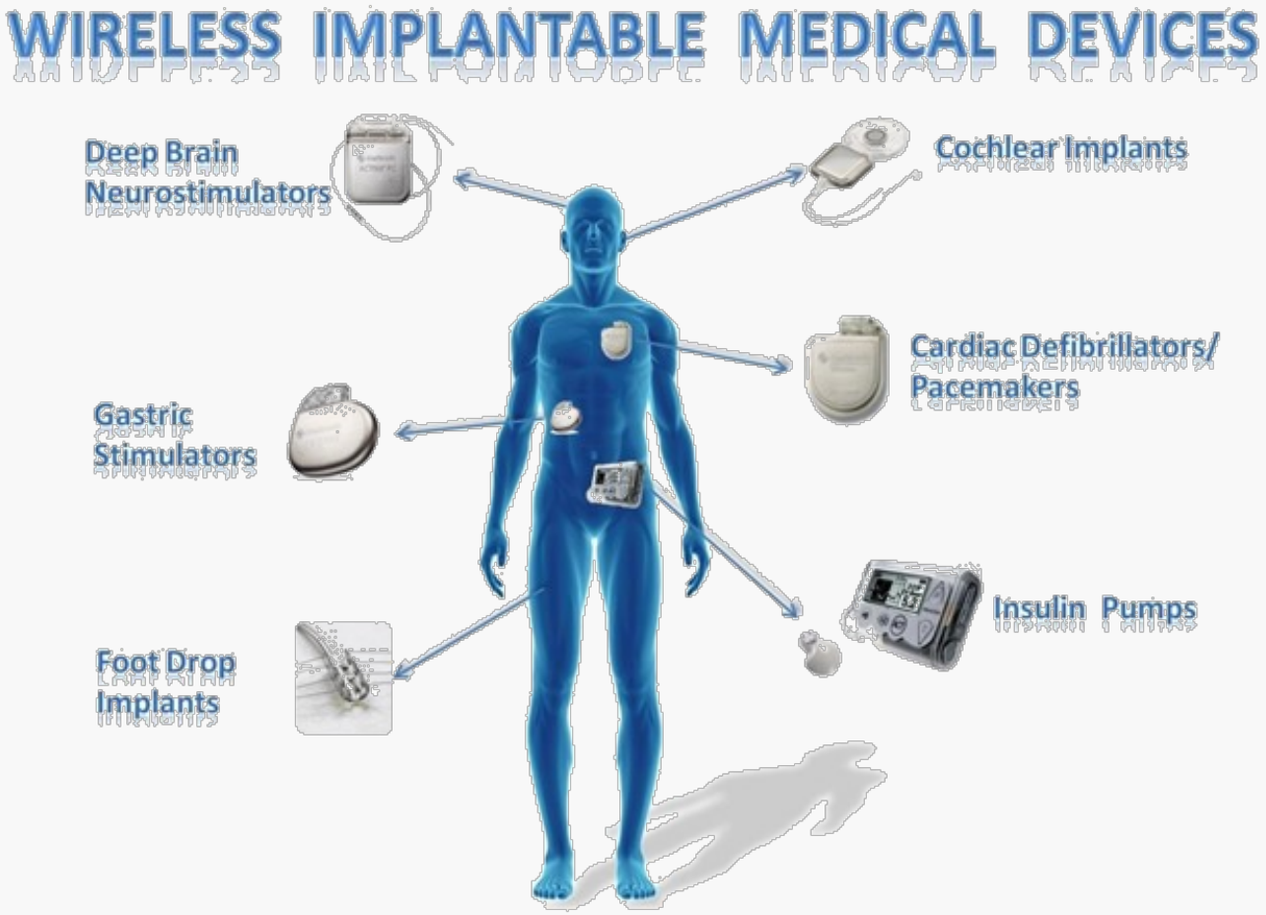
Urządzenia ubieralne i wszczepialne

- Główne trendy:
  - Body area networks – sieci monitorujących czujników
  - Urządzenia wszczepialne – ratujące życie (np. rozruszniki, dozowniki leków) lub monitorujące stan pacjenta
  - Urządzenia dedykowane
    - Medyczne
      - Dla konkretnych chorób (cukrzyca, choroby serca itp.)
    - Niemedyczne
      - Monitorujące sen, sportowe, monitorujące / nadzorujące dzieci i osoby starsze

http://www.ehealthnews.eu/images/stories/pdf/tentechnologieswhichcouldchangeourlives.pdf

Ten technologies which could change our lives: Potential impacts and policy implications

Urządzenia ubieralne i wszczepialne

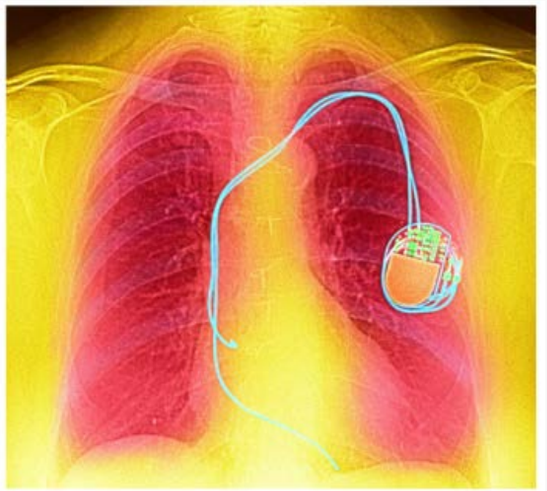


Is hacking implanted medical devices next big cyber crime?

https://null-byte.wonderhowto.com/forum/is-hacking-implanted-medical-devices-next-big-cyber-crime-0149205/

Urządzenia medyczne

- FDA
  - Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software
- HIMSS oraz American College of Clinical Engineering (ACCE), National Electrical Manufacturers Association (NEMA),
  - Manufacturer Disclosure Statement for Medical Device Security (MDS^2)
- NCHICA - North Carolina Healthcare Information & Communications Alliance, Inc. (NCHICA)

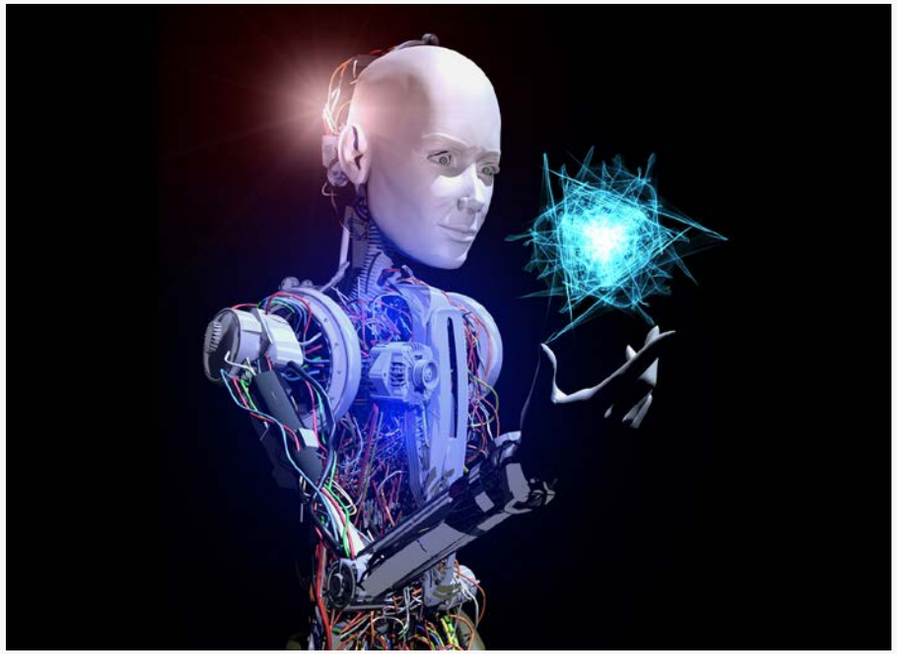


Sztuczna inteligencja oraz komputery kwantowe

Preparing for the Quantum Future: Setting Global Security Standards to Make Us Quantum-Safe:

- United States Government National Security Agency (NSA)
- United Kingdom's Communications Electronics Security Group (CESG)

https://cloudsecurityalliance.org/download/applied-quantum-safe-security/



http://www.ibtimes.co.uk/google-boasts-quantum-computing-breakthrough-first-display-real-world-use-1571823

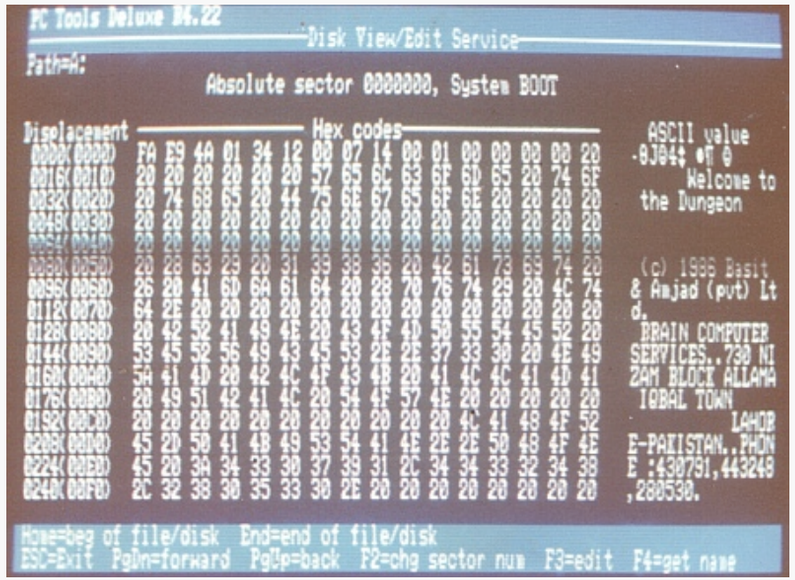
Zagrożenia i szanse

1) Bezpieczeństwo danych (nowe sposoby deszyfracji)
2) Sztuczna inteligencja wykrywająca problemy z zabezpieczeniem
3) Nadzór na AI
4) Rozwój QC

Przykłady problemów

Fakty

Pierwszy wirus komputerowy, **Brain**, został napisany przez dwóch braci, Pakistańczyków Basit Farooq Alvi oraz Amjad Farooq Alvi, z Lahore, Punjab z Pakistanu. Wirus to program który miał chronić ich własne **oprogramowanie medyczne** przed nielegalnym kopiowaniem.



Źródło Wikipedia (EN)

```
Welcome to the Dungeon (c) 1986 Basie & Amends (pvt) Ltd
VIRUS_SHOE RECORD V9.0 Dedicated to the dynamic memories
of millions of viruses who are no longer with us today -
Thanks GOODNESS!! BEWARE OF THE er..VIRUS : this program
is catching program follows after these
messages....$#@%$@!!
```

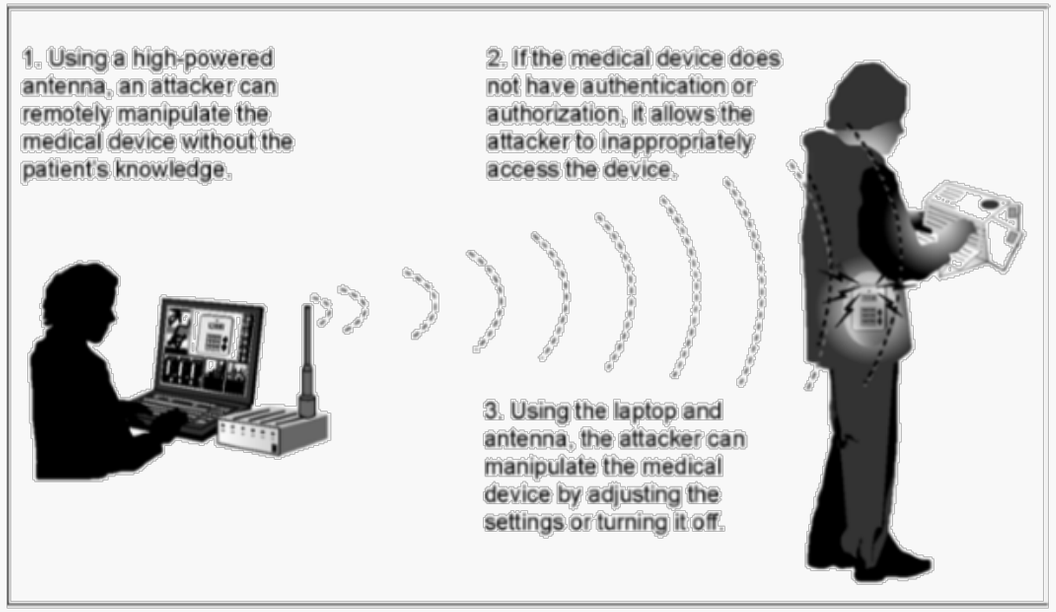
Zdjęcie zawiera (1) zapis w hex sectora boot dyskietki (A:) zawierający pierwszy wirus PC, Brain, (2) urzyto PC Tools Deluxe 4.22, narządzia do zarządzania plikami i edytor niskiego poziomu (3) PC z procesorem 8088 działającym przy 8 MHz oraz 640 Kb pamięci RAM (4) karta graficzna to CGA (4 colours at 320x200)

Fakty

- Prawie 300 000 ludzi otrzymuje bezprzewodowo komunikujące się urządzenia wszczepialne w USA
- Prawie 2,5 mln ludzi posiada IMD (Implantable Medical Devices)
- Istnieją już zdefiniowane problematyczne urządzenia (z udowodnionym dostępem dla nieupoważnionych osób)
  - Sprawdzenie bezpieczeństwa przez U.S. Homeland Security Departament wykazało 400 dziur w bezpieczeństwie urządzeń IMD (rok 2013)

http://www.slate.com/articles/technology/future_tense/2015/03/implantable_medical_devices_hacking_who_does_the_autopsy.html
http://www.cbsnews.com/news/u-s-officials-warn-medical-devices-are-vulnerable-to-hacking/
http://www.gao.gov/assets/650/647767.pdf

Figure 4: Example of Intentional Unauthorized Access of a Medical Device



Source: GAO.

Nasze rozwiązanie

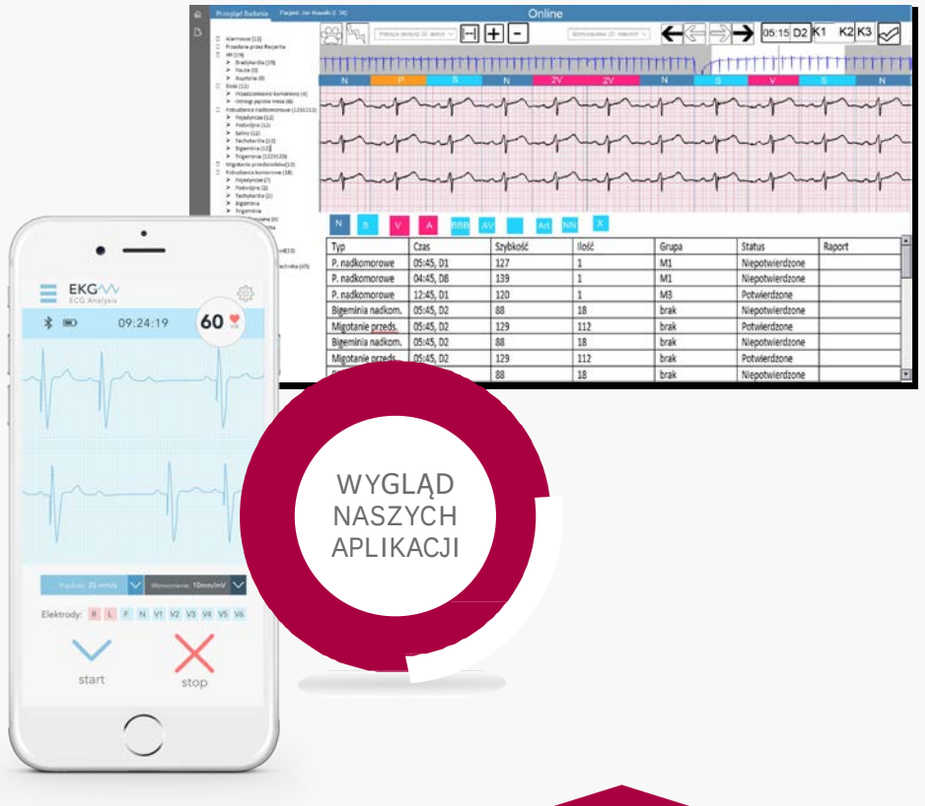
Aplikacja współpracuje z 1-12 odprowadzeniowymi urządzeniami.

Wdrożone algorytmy interpretujące badanie.

Całkowicie mobilne rozwiązanie (Android, IOS, Windows).

Wersja działająca na komputerach PC (powstaje wersja Mac OSX).

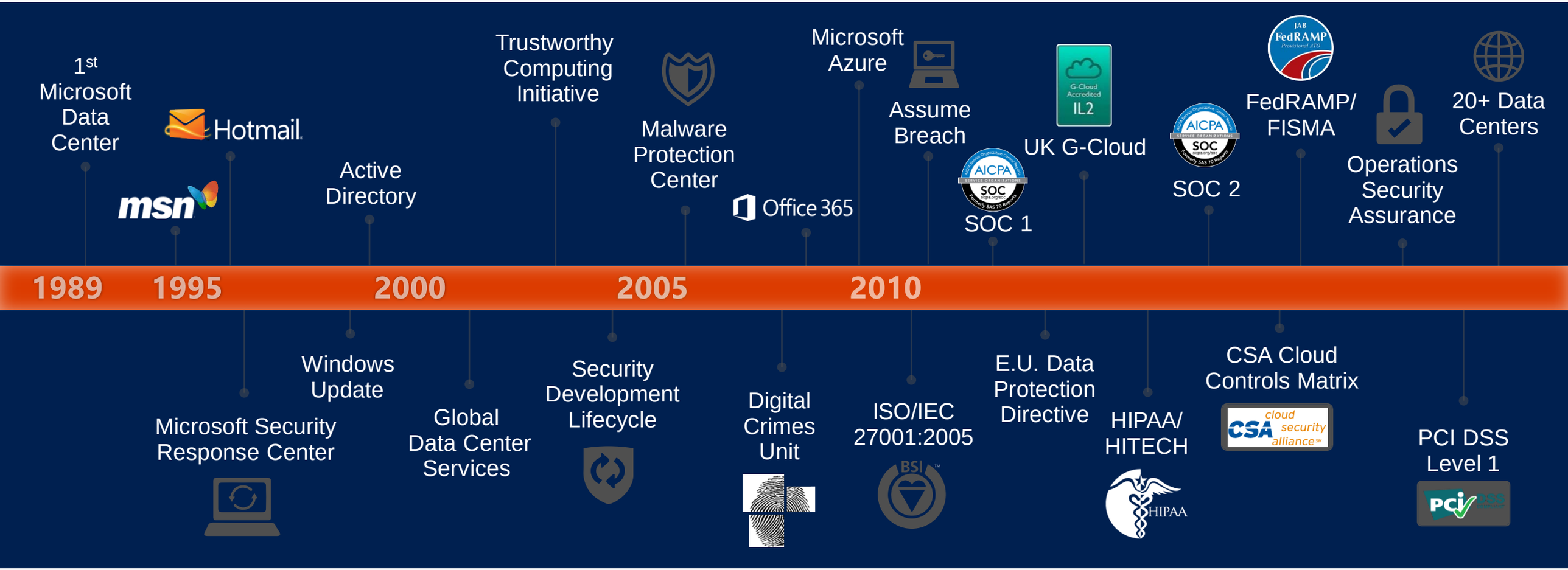
Szczegółowe raporty z przeprowadzonych badań.



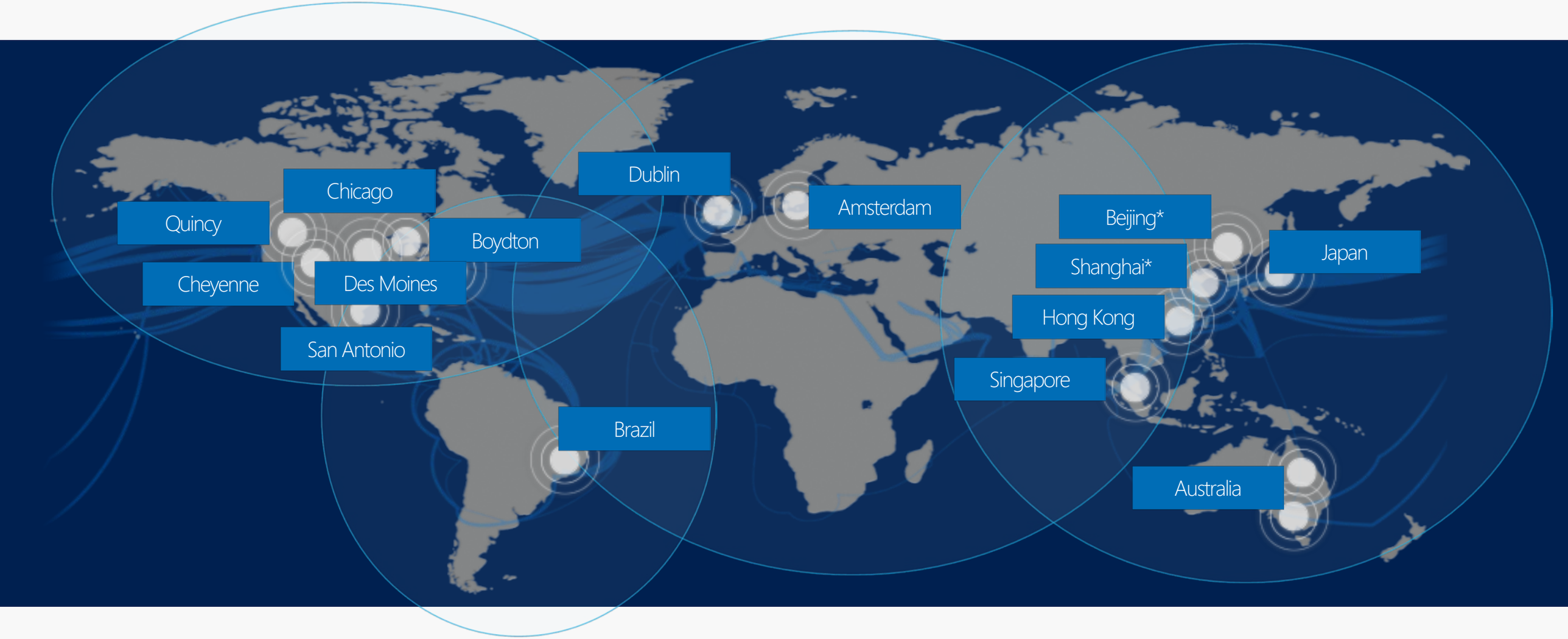
SYSTEM mHEALTH ECG

Sprzęt medyczny

Certyfikaty



Ilość serwerów



*operated by 21Vianet

Zespół

WIDZIMY PRZYSZŁOŚĆ W TWOIM ZDROWIU

Mateusz Kierepka
CEO MedApp

Współzałożyciel MedApp oraz pomysłodawca pionierskich technologii i rozwiązań będących motorem rozwoju Spółki.

Ekspert w obszarze telemedycyny z 20-letnim międzynarodowym doświadczeniem w branży IT.

Pracował przy wdrażaniu nowatorskich projektów biomedycznych.

Tomasz Kuciel
VP MedApp

Menadżer z 20-letnim doświadczeniem w zarządzaniu obszarem marketingu, sprzedaży i rozwoju biznesu.

W przeszłości pracował na stanowiskach manadżerskich prowadząc duże projekty w firmach telekomunikacyjnych (m.in. w Orange - projekt neostrada, TVoIP).

Ekspert w branży telekomunikacyjnej i elektronicznej wymiany danych (EDI).

Ralf Saykiewicz
Member of the Supervisory Board

Konsultant technologiczny z 20 letnim międzynarodowym doświadczeniem w projektach medycznych wielkiej skali.

Ekspert w dziedzinie modernizacji procesów firmy obejmujących zdrowie, logistykę, transport i produkcję.

Był odpowiedzialny za największe projekty dla US Department of Defense Military Health Services (DoD MHS), the US Department of Veterans Affairs (VA) wykonywane wspólnie z HP, Deloitte, IBM, Leidos.

Mateusz Kierepka
(+48) 533 306 116

mateusz.kierepka@medapp.pl

skypeid: kierepka

twitter.com/mkierepka

facebook.com/MedAppSA

Dobrego Pasterza 122A,
31-416 CRACOW, POLAND
www.medapp.pl