

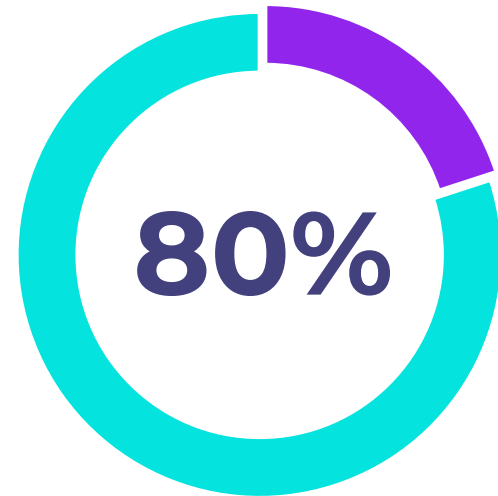
# Wspólnie złammy MFA oparte o SMS i natychmiast wprowadźmy coś lepszego

Krzysztof Gózdź – Sales Manager, Secfense, [krzysiek@secfense.com](mailto:krzysiek@secfense.com)

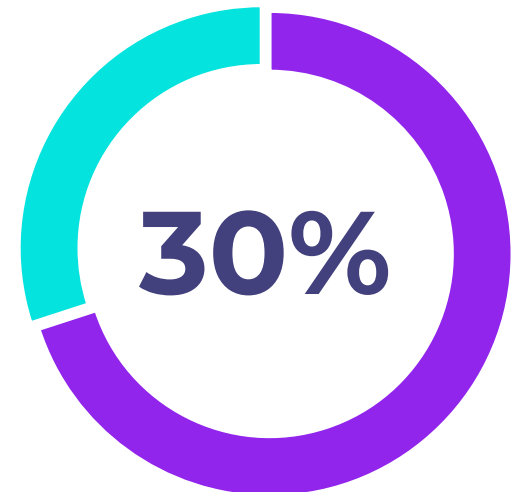


# MFA – dlaczego?

## 1. Statystyki



Incydentów zaczyna się od przejęcia konta



Udanych włamań pochodzi z wewnątrz organizacji

## 2. Regulacje

## 3. Orzecznictwo

# MFA – dlaczego?

## 1. Statystyki

## 2. Regulacje

## 3. Orzecznictwo

UKNF | URZĄD  
KOMISJI  
NAZORU  
FINANSOWEGO

Warszawa, 23 stycznia 2020 r.

Komunikat Urzędu Komisji Nadzoru Finansowego  
dotyczący przetwarzania przez podmioty nadzorowane informacji w chmurze obliczeniowej  
publicznej lub hybrydowej

### I. Definicje

- 20) **MFA** – **Multi Factor Authentication**, metoda wieloskładnikowego uwierzytelniania;
- 21) **CPD** – centrum przetwarzania danych;
- 22) **SIEM** – Security Information and Event Management, system do zarządzania informacją i zdarzeniami bezpieczeństwa;
- 23) **ujawnienie informacji** – bez uszczerbku dla rozumienia przepisów prawa bezwzględnie obowiązujących, oznacza sytuację, podczas której informacje są przetwarzane w chmurze obliczeniowej:
  - a) w sposób nieszyfrowany albo
  - b) w sposób zaszyfrowany „at rest” lub „in transit”, ale dostęp do kluczy szyfrujących i szyfrowanej tymi kluczami informacji posiada albo może posiadać dostawca usług chmury obliczeniowej lub jego poddostawca w łańcuchu outsourcingowym.



Bruksela, dnia 24.9.2020 r.  
COM(2020) 595 final

2020/0266 (COD)

Wniosek

### ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające  
rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 oraz (UE) nr  
909/2014

(Tekst mający znaczenie dla EOG)

Artykuł 8

*Ochrona i zapobieganie*

4. W kontekście ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 5 ust. 1, podmioty finansowe:
  - d) **wdrażają polityki i protokoły dotyczące silnych mechanizmów uwierzytelniania**, oparte na odpowiednich normach i specjalnych systemach kontroli, aby uniemożliwić dostęp do kluczy kryptograficznych, dzięki którym dane szyfruje się na podstawie wyników zatwierdzonych procesów klasyfikacji danych i oceny ryzyka;

# MFA – dlaczego?

## 1. Statystyki

## 2. Regulacje

## 3. Orzecznictwo

10:23  
24/3/2023

### Okradziona “na zdalny pulpit” nie musi spłacać 174 000 PLN. Zapadł wyrok.

Autor: Marcin Maj |

Tagi: ataki, banki, fraud, pieniądze, pożyczki, sąd, socjotechnika, spoofing, wyroki

Złodzieje dostali się na konto bankowe kobiety bo — podszywając się pod pracowników banku — przekonali ją, że powinna zainstalować aplikację QuickSupport, która pozwala na zdalną kontrolę komputerem. W imieniu ofiary wzięli pożyczkę i wyprowadzili pieniądze przelewami. Takich ofiar w Polsce są setki. Czy muszą spłacać pożyczkę? I ma znaczenie, że ich nieostrożność przyczyniła się do wyłudzeń?

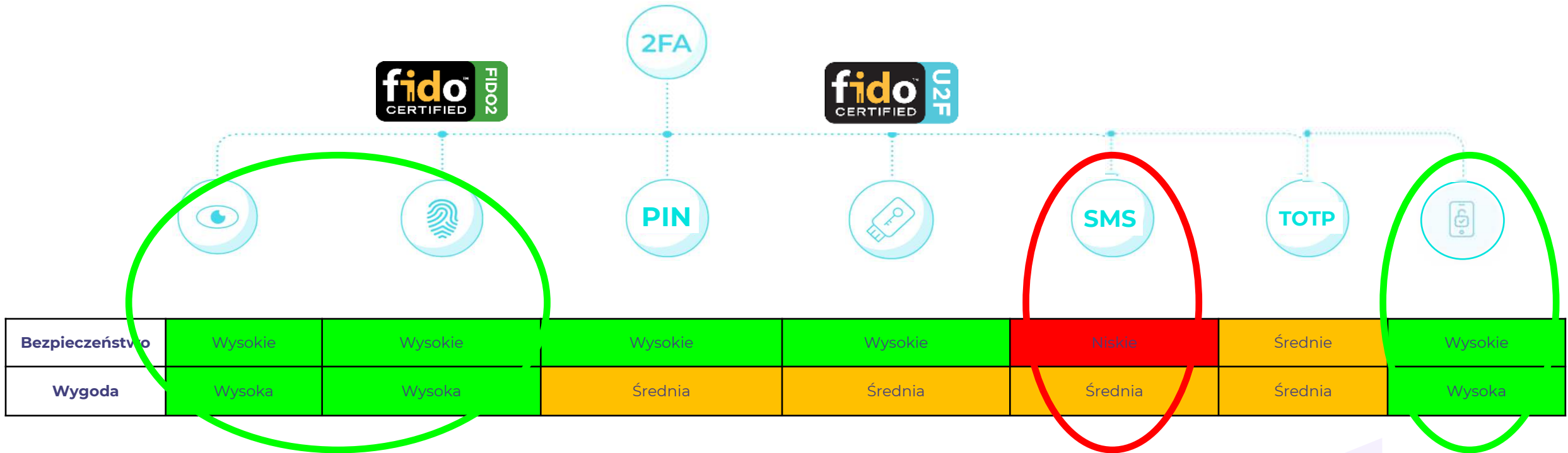
Źródło: Niebezpiecznik

# Różne typy 2FA w MFA

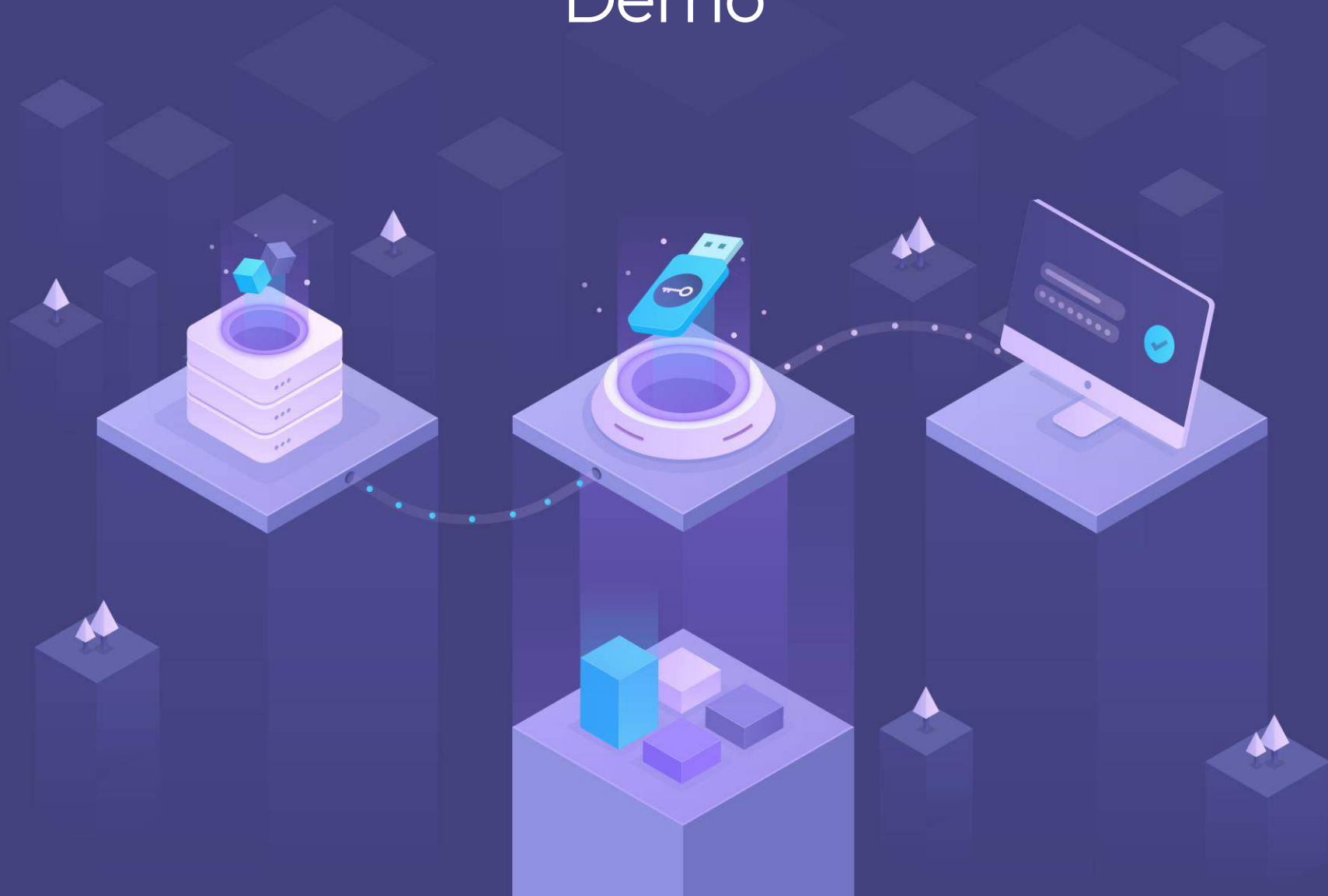


Bezpieczeństwo	Wysokie	Wysokie	Wysokie	Wysokie	Niskie	Średnie	Wysokie
Wygoda	Wysoka	Wysoka	Średnia	Średnia	Średnia	Średnia	Wysoka

# Różne typy 2FA w MFA



# Demo



# Silne uwierzytelnianie - jak je wprowadzić?



## Podejście tradycyjne – modyfikacja wszystkich aplikacji

- Ludzie?
- Firmy?
- Technologia?
- Czas?
- Ryzyka?



## Podejście Secfense – bazujące na brokerze

- Bez modyfikacji ochranianych aplikacji
- Szybko i łatwo
- Na masową skalę
- W sposób komfortowy dla użytkowników



## Jak to działa?



### Administrator:

1. Instalacja sprzętu, oprogramowania bądź skorzystanie z usługi „w chmurze”
2. Przekierowanie ruchu do aplikacji
3. Automatyczna nauka sposobu logowania poszczególnych aplikacji

### Użytkownicy:

4. Wybór i dodanie drugiego składnika uwierzytelniania

# Demo

