

Zhackowany umysł

Jak konstrukcja mózgu
sprzyja hackerom

O mnie

- Psycholog, terapeuta TSR (+ dziennikarstwo, copywriting)
- Fanka F1 i szydełkowania
- Od 2021 - Web Developer
- Fascynuje mnie cybersecurity
- <https://www.linkedin.com/in/lena-sedkiewicz/>
- <https://msedkiewicz.pl/>



Słowo o “**leniwym**” mózgu



<https://pixabay.com/photos/red-bellied-black-snake-snake-animal-6749361/>

“Leniwy” mózg

- Daniel Kahnemann - mamy “dwa mózgi” (dwa systemy reagowania)
- System 1: automatyczny
 - Przetwarza informacje poza świadomością (“intuicja”, “gut feeling”)
 - szybki
- System 2: kontrolowany
 - Wymaga naszego zaangażowania, świadomości
 - wolniejszy

“Leniwy” mózg

- System 1: automatyczny
 - Sytuacje zagrożenia (walka, ucieczka, zamrożenie)
 - Czasem - dużą rolę grają emocje
 - Nawyki
- System 2: kontrolowany
 - Świadome podejmowanie decyzji (“Pójdę schodami, dla zdrowotności”)
 - Rozmowy, dyskusje

“Leniwy” mózg

- Sytuacje społeczne - potrafią uruchomić system automatyczny



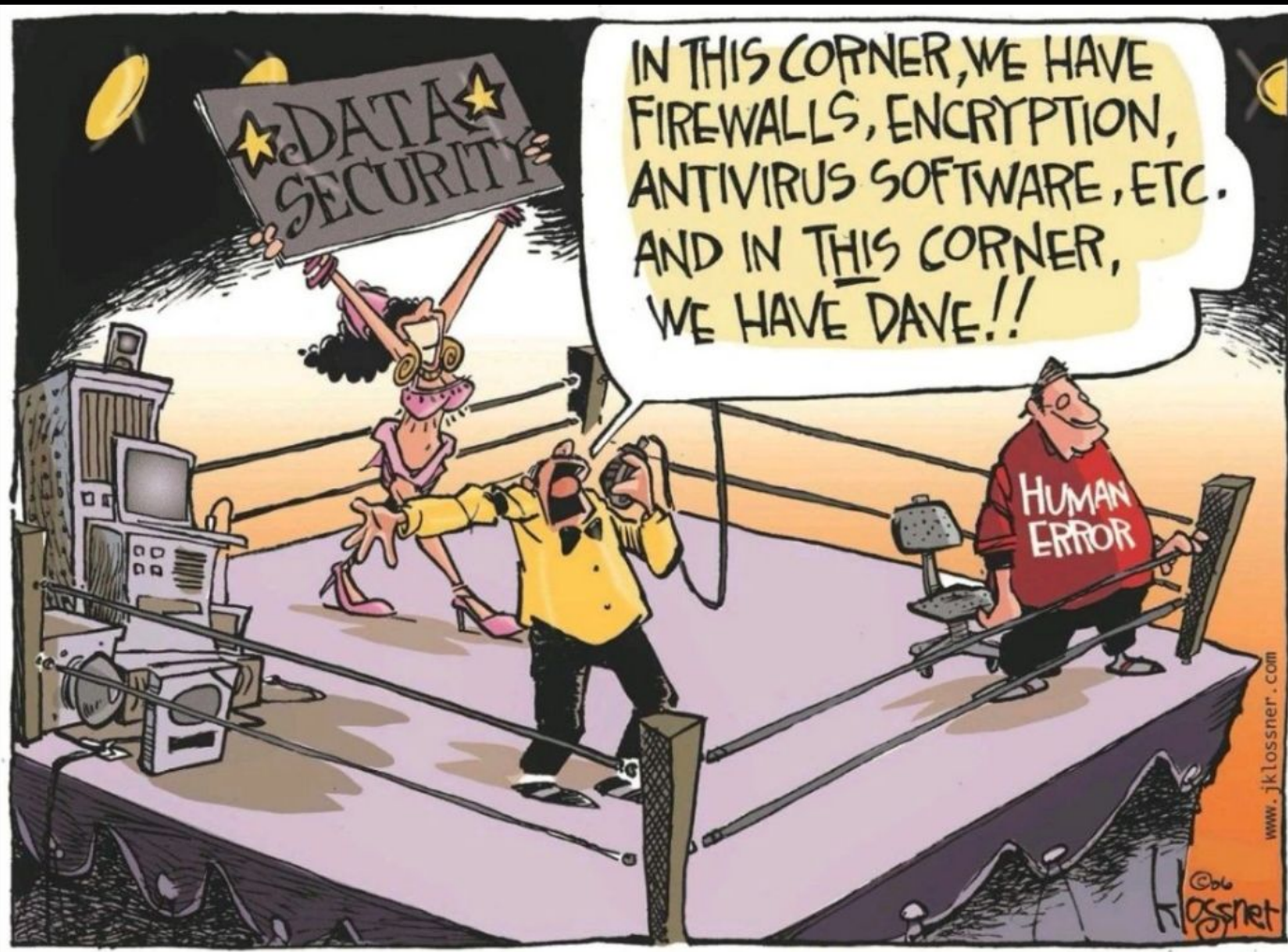
Zdrada **“zdrowego”**
rozsądku



**NIECNY
ZŁOCZYŃCA**

UŻYSZKODNIK

**OGARNIĘTY
SEKURAK**



Kim jest **Dave**?



<https://pixabay.com/photos/mirror-tree-fairytale-reflection-4433230/>

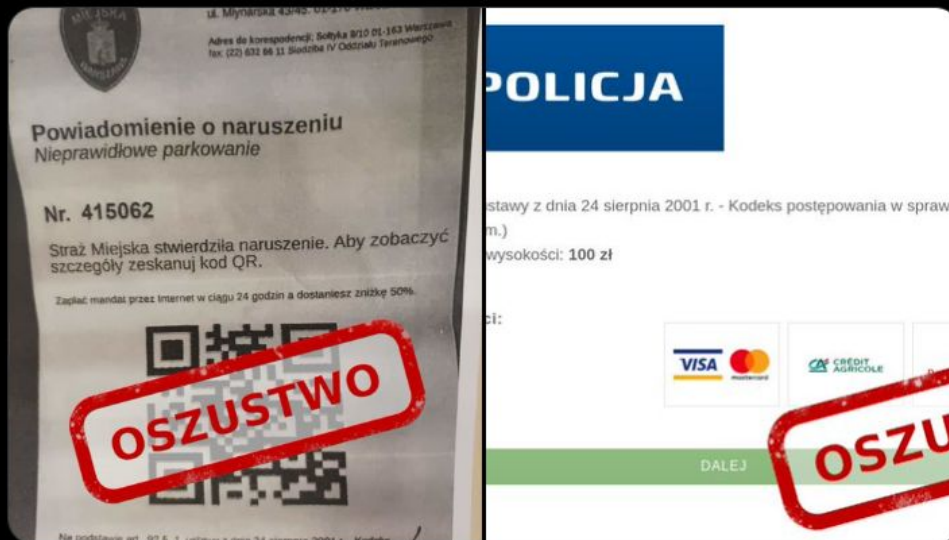
Każdy z nas...

- ... korzysta w myśleniu z systemu automatycznego i kontrolowanego, czyli korzysta z tego, co “wypluwa” mózg na bazie:
 - wychowania i innych doświadczeń społecznych
 - przekonań / schematów myślenia
 - obecnej sytuacji (która może sprzyjać wykorzystaniu jednego bądź drugiego systemu)
- Niektórzy mogą być bardziej podatni na to, co “wypluwa” mózg, inni mniej, jednak **podatny jest każdy!**
- Czyli: każdego da się zhackować ;(

Czasami cyberprzestępców spotkacie też na ulicy.

!! Razem z @CBZCgovPL ostrzegamy przed kampanią z wykorzystaniem QR kodów.

🚗 Za szybami samochodów znajdują się nieprawdziwe powiadomienia o nieprawidłowym parkowaniu wystawione rzekomo przez Straż Miejską.



To o czym będzie?

Socjotechnika? Phishing?

- Tak, to bardzo poważne wektory ataku
- Często bazują na niewiedzy i / lub emocjach (system automatyczny)
 - Telefon z banku - kradną Ci pieniądze
 - Nigeryjski książę / żołnierz amerykański - poczucie bycia wybranym / potrzebnym
- Jednak ich popularność leży głębiej niż “tylko” brak wykształcenia czy reagowanie na bazie emocji / niespełnionych potrzeb

Socjotechnika? Phishing?

- Winny jest nasz własny mózg, który “preferuje” system automatyczny (nawet nie wiemy, kiedy i jak...)
- Reakcja systemem kontrolowanym wymaga wysiłku
- Jaskiniowiec wciąż jest w każdym z nas...



Psychologia

- Wciąż się rozwija
- Nowe tezy i badania obalają stare, które żyją własnym życiem
- Tak, ma problemy z metodą badawczą (stosunkowo często)
- Sporo jednak mówi o człowieku...

Cyberryba psuje się od
głowy

Szef ma zawsze rację

A po co security? Przecież...

- Nikt nas nie zaatakował
- Są “więksi” gracze na celowniku
- To kosztuje, a efektów nie widać...
- “Ja mam używać klucza U2F?”
- Postawa osób decyzyjnych - znaczący wpływ na politykę bezpieczeństwa w firmie [1]

Szef ma zawsze rację

- Stanfordzki eksperyment więzienny
- Warunki, np. hierarchia + brak mechanizmu kontroli = szef ma zawsze rację
- Otoczenie “wymusza” pewną rolę; brak kontroli doprowadza do problemów / tragedii



https://en.wikipedia.org/wiki/Stanford_prison_experiment#/media/File:SPE1971-prisoners_in_bed_in-cell.jpg

Szef ma zawsze rację

“Po przeanalizowaniu dostępnych materiałów doszli do przekonania, że bez aktywnej roli w nakłanianiu strażników do brutalnych zachowań, bez budowania przez nich tożsamości grupowej, bez zwalczania bierności wycofujących się, mało aktywnych strażników, rozwój sytuacji w podziemiach stanfordzkiego uniwersytetu byłby zgoła odmienny.”

<https://tomwitkow.wordpress.com/2018/07/02/lucyfer-ktorego-wymyslil-zimbardo-o-konsekwencjach-stanfordzkiego-eksperymentu-wieziennego-i-skandalu-ktorego-stal-sie-obiektem/>

Skoro szef, to się zna! A w mózgu szefa...

- Efekt fałszywej unikalności (przekonanie szefa o tym, że firma jest ponadprzeciętnie dobrze przygotowana do ataku)
- Efekt fałszywego konsensusu (szef zakłada, że zgadza się z nim więcej osób niż w rzeczywistości)
- Nierealistyczny optymizm (= mniej działań przygotowawczych do ewentualnego negatywnego scenariusza)
- Szef = facet w fartuchu. A facet w fartuchu...

Szef = facet w fartuchu

- Badanie posłuszeństwa - Milgram
- “Proszę kontynuować”
- Facet w fartuchu = facet w garniturze
- Instytucja polecenia służbowego (dodatkowe narzędzia wpływu)



<https://www.quora.com/Given-the-results-of-the-Milgram-study-is-it-fair-to-judge-people-for-being-immoral-when-they-may-have-been-pressured-and-psychologically-tricked-into-following-orders>

<https://youtu.be/QIDRmVuGwK4?t=16343>

Ciulowa, by nie rzec inaczej
organizacja pracy



Andrzej Dyjak • 1.

Bezpieczeństwo Aplikacji i DevSecOps • Właściciel Bezpi...

18 min •



Takie cukierki można znaleźć w prawdziwych aplikacjach.

Kto robił audyty kodu ten się w cyrku nie śmieje. ☐



r/ProgrammerHumor • Posted by u/aarontbarratt 4 hours ago



foundThisGemInOurCodebaseToday

Meme

nsfw

OC

```
# sanitize a string ready for use in a database
def sanitize(text):
    return text
```



z Bezpieczny Kod

Lęk przed oceną?

- Pisanie kodu / wdrażanie jakichkolwiek rozwiązań w IT - czas!
- A gdy manager generuje presję...
- Lęk przed oceną
 - Wydajności
 - Tempa pracy
 - Dowiezionych sprintów
- Redukcja czasu na stosowanie dobrych praktyk (m.in. security)
- **Ma działać!**
- Stawka - zachowanie pracy

Rozmyta odpowiedzialność - scenariusz

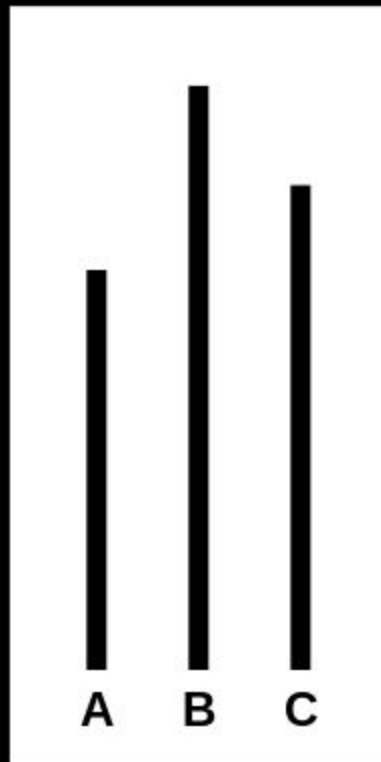
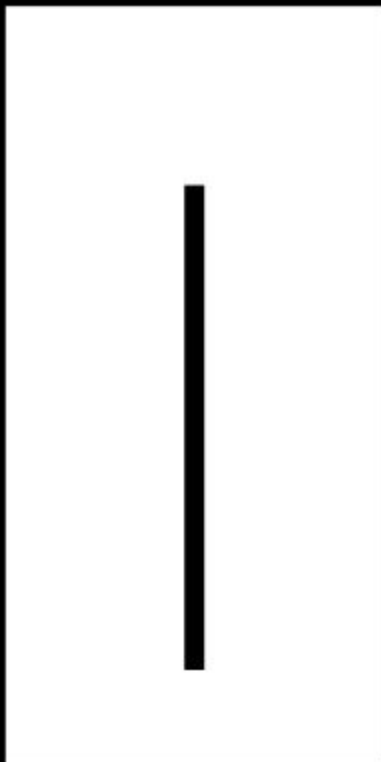
- Masz pomysł na zmianę w obszarze security
- Manager mówi: wpisz do backlogu, omówimy to w gronie managerów, z szefem, z innymi członkami zespołu
- Przypominasz o przedyskutowaniu zmian. Raz, drugi, trzeci... Niby coś drgnęło, ktoś się zastanawia, ktoś
- Twój backlog świeci się na czerwono - zadania high priority, ale nie z security
- Dochodzi do ataku.
- Kto jest winny?

Rozmyta odpowiedzialność

- Praca w zespole w szkole? Jedna osoba robi, inni korzystają
- W jakimś stopniu podobnie bywa w życiu zawodowym...
- Próżniactwo społeczne – obecność w grupie rozmywa odpowiedzialność
- Winnego nie ma...
- ...zawinił system?
- ...albo sposób myślenia - jestem w grupie, nie muszę robić wszystkiego, są inne osoby decyzyjne, ja się nie wtrącam

O spotkaniach, które mogły
być **mailem**

Jak często spotkania firmowe mają
potwierdzić z góry założoną tezę?



https://pl.wikipedia.org/wiki/Plik:Asch_experiment.svg

Konformizm

- 75% przynajmniej raz ulega opinii innych
- W sytuacji gdy wszyscy podstawieni badani mówią coś niezgodnego z prawdą: 37% osób ulega, 63 % zostaje przy własnym zdaniu
- Konformizm - zmiana zachowania bądź przekonań zgodnie
- z tym, co robią / myślą inni.
- Ważniejsza jest akceptacja społeczna, zgodność niż wyrażenie własnego zdania - które mogłoby jednak zmienić kurs dyskusji...

Myślenie grupowe

„Sposób myślenia w który jednostka angażuje się gdy tendencja do szukania zgodności w spójnej grupie jest tak dominująca, że przeważa nad realistyczną oceną alternatywnych opcji wyboru.” (Irving Janis, 1971).

- Iluzja niezniszczalności (wiara w moralność grupy)
- Iluzja niezniszczalności prowadzi do przeceniania pozycji grupy (jesteśmy najważniejsi)
- Racjonalizacja (stereotypowe postrzeganie osób o odmiennych poglądach)
- Zawężenie procesów myślowych

Myślenie grupowe. Punkt, gdzie zaczyna się katastrofa

- Presja – w kierunku uległości
 - Autocenzura
 - Iluzja jednomyślności
 - Działają „Strażnicy umysłu”
-
- Dodajmy jeszcze m.in. dyrektywne przywództwo, izolację grupy oraz niechęć do pogłębienia odmiennych stanowisk, i...

Spoiler alert!



Kult Cargo

- „Ptaki niebios”
- Nowa Gwinea, lata 30.
- Żołnierze wypakowują z „brzucha” stalowej istoty skrzynie ze sprzętem, jedzeniem, innymi dobrami użytkowymi. Tworzą bazy wojskowe.
- Myślenie tubylców: jeśli będziemy robić to samo co „biali ludzie”, to duchy przodków ześlą nam cargo.
- Kult Cargo - wyciąganie niewłaściwych wniosków na bazie dostępnych przesłanek [2]

Zagrożenie stereotypem

- Destrukcyjna w skutkach obawa, w obliczu negatywnego stereotypu, że ktoś zostanie oceniony w jego oparciu



Negocjacje z **Użyszkodnikiem**

Tragedia wspólnego pastwiska

- Sprawa dotycząca nas wszystkich staje się sprawą, którą nikt się nie przejmuje. Przykładowo:
 - Segregacja śmieci
 - Oszczędzanie wody / energii elektrycznej
 - Dbanie o wspólną przestrzeń - parki, ulice, przystanki
 - Wymiana kopciuchów i palenie czym się da
 - Dbanie o zdrowie (bo przecież to wspólna sprawa...)
 - Cyberbezpieczeństwo

Efekt uśpienia

- Sytuacja, w której informacja pierwotnie odrzucona z pewnych przyczyn staje się wiadomością wpływającą na nasze zachowanie, ze względu na to że zapominamy przyczynę odrzucenia danej informacji
- Najpierw mamy “odbębniiony” kurs security, a po kilku miesiącach...
- “To rozwiązanie jest złe... nieeeee, chyba robię dobrze”

Umiejscowienie kontroli

- Wewnętrzne - poczucie kontroli nad tym, co się dzieje w Twoim życiu
- Zewnętrzne - poczucie, że wieloma sprawami kieruje ślepy traf / zewnętrzne siły
- Wewnętrzne poczucie kontroli sprzyja podejmowaniu zachowań prewencyjnych

Postrzeganie siebie

- Egotyzm atrybucyjny
 - Dostałam 5 - pracowałam na to. Dostałam 2 - wykładowca się uwziął
- Porównywanie się z innymi
 - Piszę kod lepiej niż Stefan
- Nierealistyczny optymizm
 - “Pomimo iż 50% małżeństw się rozpada moje na pewno przetrwa!”
- Fenomen sprawiedliwego świata - “dobrym ludziom nie przydarzają się złe rzeczy”

Tajemnica fakapów
sekuraków

How users see the programmers



How programmers see the users



Ja vs. inni - postrzeganie sytuacji

- Aktor - ja w swoim życiu, widzę czynniki zewnętrzne, które wpływają na moje nietrafione decyzje
 - Obserwator - widzę człowieka z konkretnymi cechami, który jest partaczem
-
- Z perspektywy obserwatora łatwiej oceniać Użyszkodników

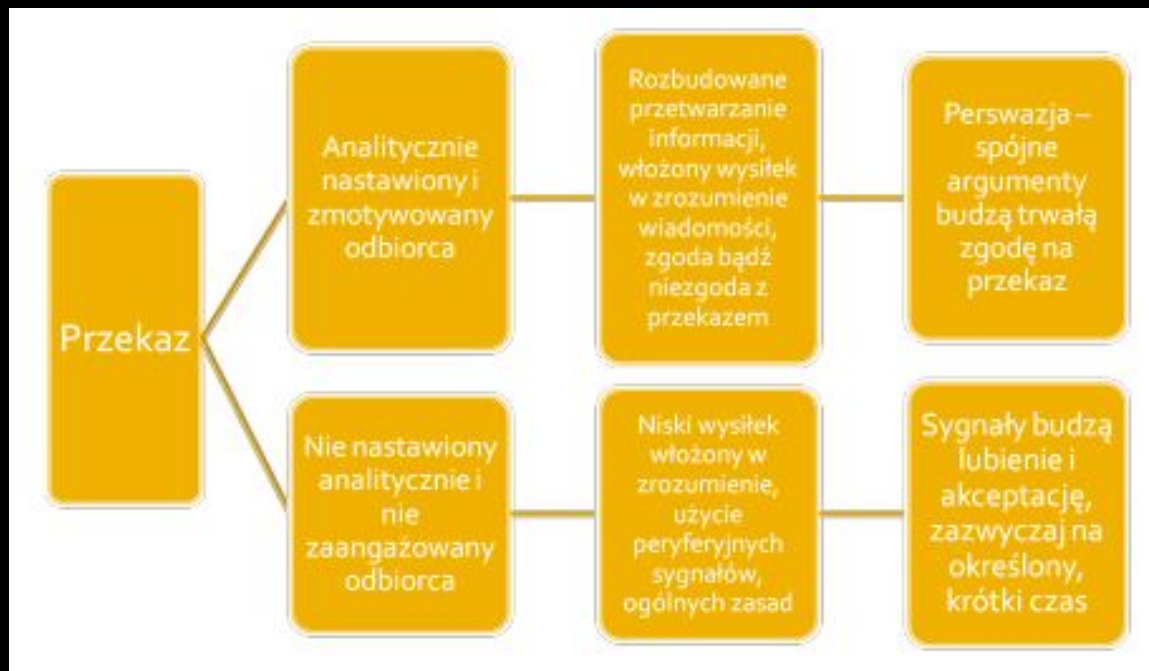
Efekt odnoszenia do siebie

- Jeśli dana informacja jest istotna dla naszej koncepcji „ja”, szybko ją przetwarzamy i dobrze ją zapamiętujemy (Higgins & Bargh, 1987; Kuiper & Rogers, 1979; Symons & Johnson, 1997).
- Dwa dni po konwersacji, przypominamy sobie lepiej to, co dotyczyło nas (co ktoś o nas powiedział, Kahan & Johnson, 1992)
- Gromadzenie i wychwytywanie wiedzy cybersecurity tam, gdzie inni “ślizgają się” po niej wzrokiem
- Wy tak macie z cybersecurity, inni nie ;)

Dwie drogi perswazji

- Perswazja – proces, w efekcie którego wysyłana wiadomość wpływa na zmianę przekonań, nastawienia bądź zachowania.
- Proces edukacji Użyszkodnika - opiera się o perswazję
- Chcemy zmienić nawyki Użyszkodnika!

Dwie drogi perswazji



Jak żyć?

1. Praca nad sobą i nad “kwestionowaniem: własnych osądów
 - a. nauka przyjmowania perspektywy drugiego człowieka (“wejście w czyjeś buty”)
2. Dostosowanie komunikatu do okoliczności
3. Zdrowy pesymizm + akceptacja porażki (lęk przed oceną / porażką paraliżuje)
4. Pokora -> Ciekawość siebie i innych

5. Nauka przeciwwstawiania się presji szefa / grupy

- a. Budowanie odporności psychicznej
- b. Szukanie sojuszników
- c. “Bunt na pokładzie”

6. Mechanizmy kontroli osób decyzyjnych / ochrony sygnalistów
7. Klarowne procesy i podział odpowiedzialności (wiem, co robię i za co odpowiadam)
8. Bardziej “pozioma” organizacja pracy (sprzyjająca wyrażaniu zdania odrębnego)
9. Zaangażowanie (“w moim interesie jest wiedzieć więcej”)
10. Przeciwdziałanie myśleniu grupowemu

10. Przeciwdziałanie myśleniu grupowemu

- Pozostanie bezstronnym / bezstronną
- Zachęcenie do krytycznej analizy; wyznaczenie „adwokata diabła”
- Okazjonalnie na czas dyskusji podzielenie grupy, by po połączeniu mogło dojść do wymiany opinii
- Przyjęcie krytyki od osób z zewnątrz – ekspertów i współpracowników
- Przed wprowadzeniem rozwiązania - zwołanie „spotkanie ostatniej szansy” aby porozmawiać o pojawiających się wątpliwościach

Dziękuję za uwagę!

<https://www.linkedin.com/in/lena-sedkiewicz/>

<https://msedkiewicz.pl/>

Przypisy + materiały

- [1] Policies, innovative self-adaptive techniques and understanding psychology of cybersecurity to counter adversarial attacks in network and cyber environments - R Montasari, A Hosseinian-Far, R Hill
- [2] Tomasz Witkowski, „Zakazana Psychologia, t. 2” (warto przeczytać wszystkie tomy Zakazanej Psychologii)
- Psychologia społeczna, David G. Myers
- Exploring social psychology, David G. Myers