ANGRY DEV

Co może zrobić złośliwy deweloper?

Adrian Sroka

Kto zazwyczaj stanowi zagrożenie dla naszych systemów?

Kto zazwyczaj stanowi zagrożenie dla naszych systemów?

Skąd może nadejść atak?

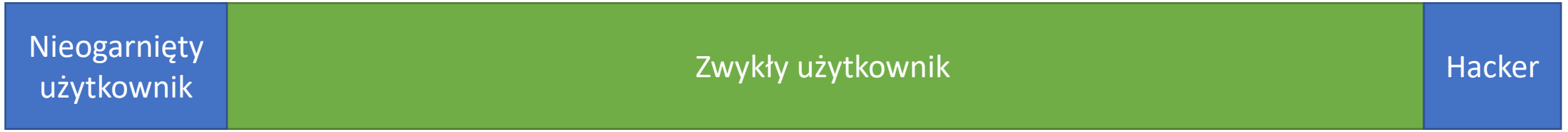
Użytkownik

- Potencjalny atakujący
- Potencjalny atakowany

Użytkownicy w oczach deweloperów

Jak to widzą deweloperzy?

Jak to wygląda naprawdę?



Skąd jeszcze może nadejść atak?

Firmy zewnętrzne

- Mają dostęp do naszych danych
- Mogą być źródłem danych lub ruchu (i to zaufanego)

Czy to wszystko?

- Brak aktora, który ma największe możliwości ataku

Deweloper?
To niemożliwe.

„Przecież go znam”

„Przecież mu płacę”

„Przecież od razu się dowiem”

„Przecież inni od razu zauważą”

„Dlaczego miałby coś takiego robić?”

Co ma deweloper?

Zaufanie

Dostęp do kodu + modyfikacje

Dostęp do danych produkcyjnych

Dostęp do danych Klientów

Dostęp do infrastruktury

Kiedy deweloper może stanowić zagrożenie?

Świadome

- Zwolnienie
- Konkurencja
- Złośliwość

Nieświadome

- Phishing
- Pomyłka

Największe zagrożenie to błędy dewelopera

Zagrożenia ze strony dewelperów

oczywiste

Drop bazy
Drop indeksów

Mitygacja:
- Deweloperzy bez dostępu do modyfikacji na bazie

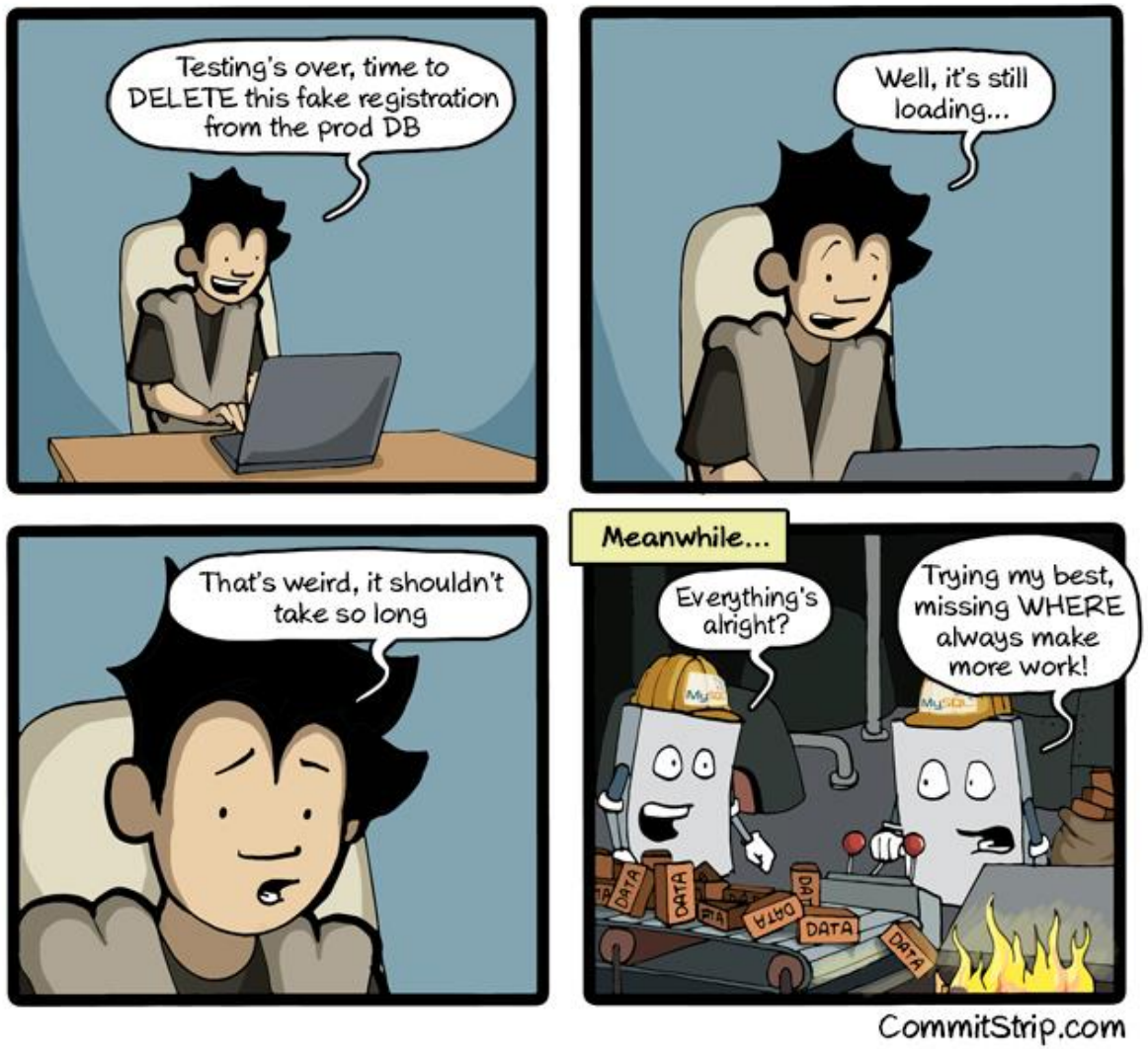
Zagrożenia ze strony dewelperów

oczywiste

Kradzież danych

Mitygacja:
- Ograniczony dostęp do danych produkcyjnych
- Anonimizacja na środowiskach DEV
- Anonimizacja logów

To za proste


Testing's over, time to DELETE this fake registration from the prod DB
Well, it's still loading...
That's weird, it shouldn't take so long
Meanwhile...
Everything's alright?
Trying my best, missing WHERE always make more work!
DATA
CommitStrip.com

Zagrożenia ze strony dewelperów

mniej oczywiste

Sekrety Klientów zawarte w zgłoszeniach błędów

Mitygacja:
- Edukacja użytkowników
- Czyszczenie sekretów

Zagrożenia ze strony dewelperów

mniej oczywiste

Wysyłka kompromitujących maili z adresów firmy

Mitygacja:
- Ukrycie sekretów produkcyjnych przed deweloperami

Zagrożenia ze strony dewelperów

mniej oczywiste

Wykorzystanie zasobów chmurowych

Mitygacja:
- Ograniczenie dostępu dla deweloperów

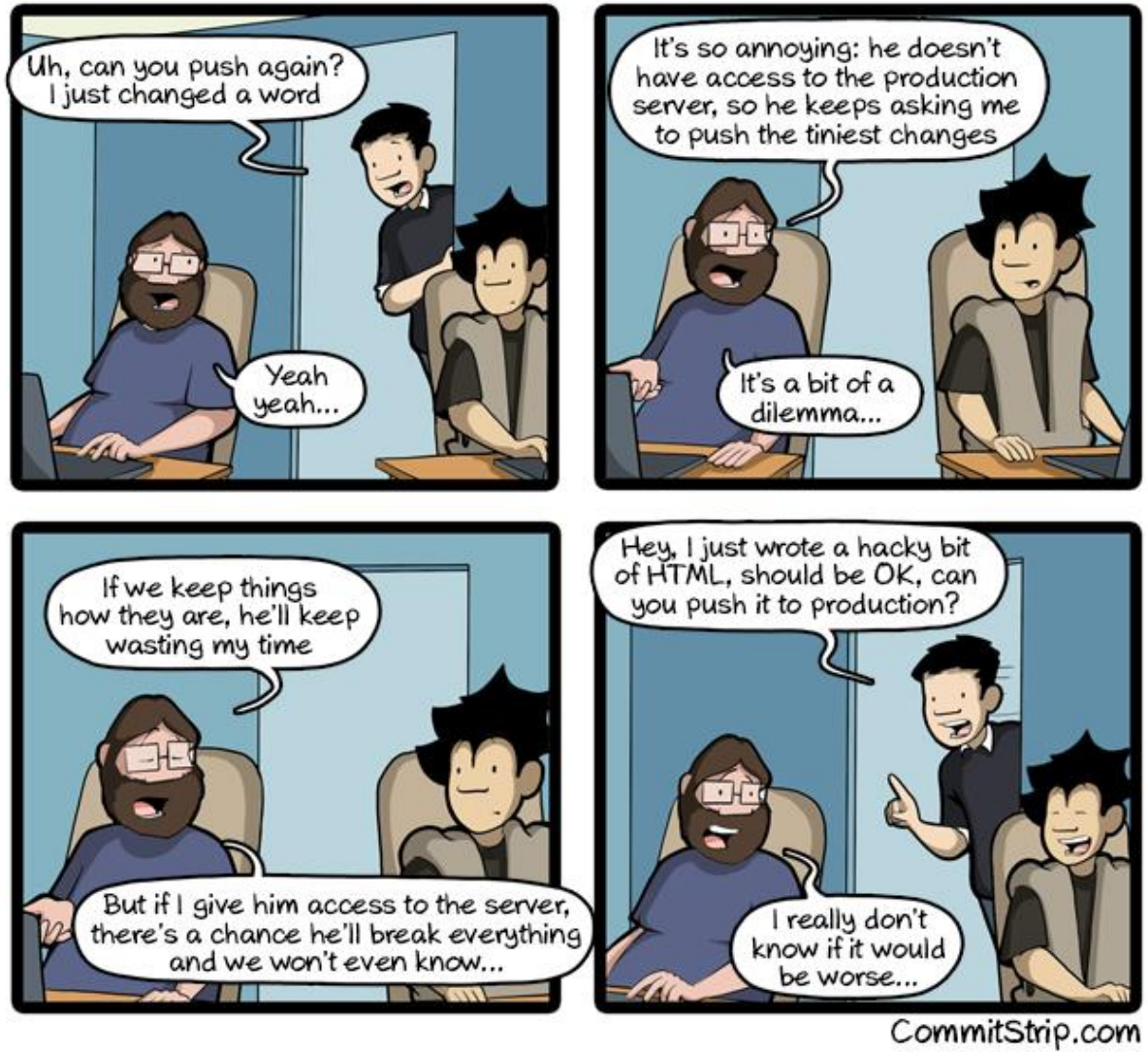
Zagrożenia ze strony dewelperów

mniej oczywiste

Modyfikacja współdzielonych zasobów – dokumentacji

Mitygacja:
- Kontrola dostępu

Może jeszcze bardziej skomplikowane



Zagrożenia ze strony dewelperów

ukryte

Backdoor

DoS bomb

Ukryte luki

Mitygacja:
- Code Review

Zagrożenia ze strony dewelperów

ukryte

Biblioteka pod prywatną kontrolą (typosquatting)

Mitygacja:
- Ocena dojrzałości bibliotek
- Code Review

Zagrożenia ze strony dewelperów

ukryte

Podmiana plików, zasobów na serwerze

Mitygacja:
- Ograniczenie uprawnień

Zagrożenia ze strony dewelperów

ukryte

Złośliwe skrypty budujące/githooki

Mitygacja:
- Code review

I wiele, wiele więcej

Wyobraźnia nas tylko ogranicza

Jak sobie z tym poradzić?

Anonimizacja

Ograniczenie uprawnień

Brak dostępu do Produkcji

Code Review

Audyt zmian

ZERO TRUST

Jak sobie z tym poradzić?

Warto być świadomym

Bez przesady

Przeprowadzić modelowanie wewnętrznych zagrożeń

Jak szybko nowy deweloper dostaje dostęp do produkcji?

Dziękuje za uwagę