PKI w praktyce

Wnioski z implementacji własnej infrastruktury certyfikatów

Prelegenci:
Krzysztof Taraszkiewicz, Jakub Szymczyk, Józef Sztabiński, Jakub Drejka

Wprowadzenie do Cyberbezpieczeństwa
Politechnika Gdańska

Agenda prezentacji

1. **Dlaczego PKI jest fundamentem bezpieczeństwa?**
2. **Czego nauczyła nas implementacja własnego CA?**
3. **Kiedy wybrać własne CA, a kiedy komercyjne rozwiązanie?**
4. **Pułapki i błędy w zarządzaniu certyfikatami**
5. **Najważniejsze wnioski dla praktyki**

Część I: Fundamenty

Dlaczego PKI jest tak ważne?

Wniosek #1: PKI to więcej niż "tylko certyfikaty"

🔑 PKI to system zaufania

- Jeden skompromitowany klucz CA = cała infrastruktura zagrożona
- Hierarchia zaufania musi być przemyślana od początku
- Backup i odtwarzanie kluczy to sprawa krytyczna

Przykład:

```
Politechnika Gdańska Root CA (4096-bit, zaszyfrowany)
├── Serwery WWW (2048-bit, krótszy okres ważności)
└── Klienci (2048-bit, różne uprawnienia)
```

Bezpieczeństwo całego systemu = bezpieczeństwo najsłabszego ogniwa

Wniosek #2: Zaufanie nie jest binarne

Różne poziomy zaufania w naszej implementacji:

Typ certyfikatu	Okres ważności	Poziom zabezpieczeń	Zastosowanie
Root CA	20 lat	Maksymalny	Fundament zaufania
Serwer	1 rok	Wysoki	Szyfrowanie komunikacji
Klient	2 lata	Średni	Uwierzytelnianie użytkowników

Kluczowy wniosek:

- Im dłuższy okres ważności → tym większe ryzyko
- Im wyżej w hierarchii → tym silniejsze zabezpieczenia
- Balans między wygodą a bezpieczeństwem

Część II: Praktyka

Wniosek #3: Formaty to nie tylko technikalia

Dlaczego formaty certyfikatów mają znaczenie:

Format	Kiedy używać	Główna lekcja
PEM	Serwery Linux, skrypty	Czytelność = łatwiejsze debugowanie
DER	Integracje Java/Windows	Kompatybilność ma swoją cenę
PKCS#12	Transport kluczy	Bezpieczeństwo > wygoda

Wybór formatu to decyzja architektoniczna, nie techniczna

Część III: Wybory strategiczne

Własne CA vs rozwiązania komercyjne

Wniosek #4: Nie ma rozwiązania uniwersalnego

Macierz decyzyjna oparta na naszym doświadczeniu:

Scenariusz	Własne CA	Let's Encrypt	Komercyjne CA
Nauka/Lab	✅ Idealne	❌ Zbyt proste	❌ Drogie
Startup	❌ Za trudne	✅ Optymalne	❌ Niepotrzebne
Korporacja	⚠️ Wymaga ekspertów	❌ Ograniczone	✅ Wsparcie
Usługi publiczne	❌ Brak zaufania	✅ Akceptowalne	✅ Preferowane

Kluczowe pytania przy wyborze:

1. **Kto będzie zarządzał infrastrukturą?**
2. **Jakie są koszty całkowite (TCO)?**
3. **Czy potrzebujemy niestandardowych rozszerzeń?**

Wniosek #5: Automatyzacja to konieczność, nie opcja

Co działało ręcznie vs co wymaga automatyzacji:

📝 **Działało ręcznie** (projekt edukacyjny):

- Generowanie pojedynczych certyfikatów
- Weryfikacja podstawowa
- Konwersje formatów

🤖 **Wymaga automatyzacji** (środowisko produkcyjne):

- Odnawianie certyfikatów
- Monitoring dat wygaśnięcia
- Zarządzanie CRL (Certificate Revocation Lists)
- Backup i recovery

Ręczne zarządzanie certyfikatami w dużej firmie to sposób na katastrofę

Część IV: Pułapki i błędy

Wniosek #6: Najczęstsze błędy w PKI

1. Błędy bezpieczeństwa:

❌ Niezaszyfrowane klucze prywatne
❌ Słabe hasła do kluczy CA
❌ Zbyt długie okresy ważności
❌ Brak backupu kluczy prywatnych

2. Błędy operacyjne:

❌ Zapomnienie o odnowieniu certyfikatów
❌ Nieprawidłowe uprawnienia plików
❌ Brak monitoringu CRL
❌ Nieprawidłowa konfiguracja rozszerzeń

3. Błędy architektoniczne:

❌ Zbyt płaska hierarchia CA
❌ Mieszanie środowisk (test/prod)
❌ Brak procedur odwołania certyfikatów

Wniosek #7: Weryfikacja to podstawa zaufania

Warstwy weryfikacji:

1. **Kryptograficzna** - czy podpis jest prawidłowy?
2. **Czasowa** - czy certyfikat jest aktualny?
3. **Hierarchiczna** - czy łańcuch zaufania jest kompletny?
4. **Funkcjonalna** - czy certyfikat może być użyty do danego celu?
5. **Polityczna** - czy certyfikat nie został odwołany?

Lekcja: Weryfikacja to proces, nie pojedyncza operacja

Część V: Praktyczne wnioski

Wniosek #8: Lista kontrolna dla PKI

✅ Przed implementacją:

- [ ] Zdefiniowana polityka bezpieczeństwa
- [ ] Przemyślana hierarchia CA
- [ ] Procedury zarządzania kluczami

✅ Podczas implementacji:

- [ ] Silne hasła i szyfrowanie kluczy
- [ ] Prawidłowe uprawnienia plików
- [ ] Odpowiednie okresy ważności
- [ ] Testowanie w środowisku izolowanym

✅ Po wdrożeniu:

- [ ] Monitoring dat wygaśnięcia
- [ ] Procedury awaryjne
- [ ] Dokumentacja i szkolenia

Część VI: Przyszłość PKI

Wniosek #9: PKI ewoluuje

🔮 **Automatyzacja** (ACME protocol, Let's Encrypt)
🔮 **Krótsze okresy ważności** (90 dni → standard)
🔮 **Post-quantum cryptography** (przygotowania na komputery kwantowe)
🔮 **Certificate Transparency** (publiczne logi certyfikatów)
🔮 **Blockchain-based PKI** (decentralizacja CA)

Co to oznacza dla praktyków:

- Mniej ręcznej pracy, więcej automatyzacji
- Nacisk na monitoring
- Potrzeba ciągłego uczenia się nowych technologii

Kluczowe przesłanie wykładu

💡 Główne wnioski:

1. **PKI to fundament** - bez zrozumienia PKI nie ma cyberbezpieczeństwa
2. **Praktyka ≠ Teoria** - implementacja ujawnia prawdziwe wyzwania
3. **Nie ma rozwiązań uniwersalnych** - każdy przypadek wymaga analizy
4. **Automatyzacja to konieczność** - ręczne zarządzanie to droga do błędów
5. **Bezpieczeństwo to proces** - nie jednorazowa konfiguracja

Materiały uzupełniające

- **PKI-tutorial.readthedocs.io** - praktyczne przykłady

Dziękujemy za uwagę