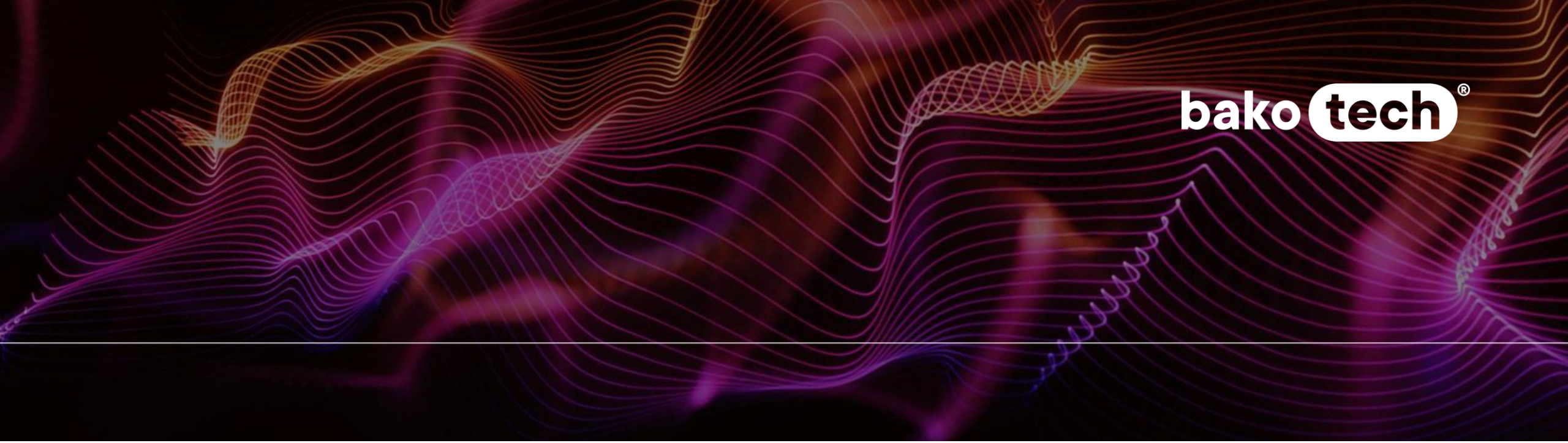


Damian Gołuch

Business Unit Manager | Product Manager

Jak skutecznie zabezpieczyć infrastrukturę krytyczną z pomocą nowoczesnych narzędzi i procedur

Jak dobrać nowoczesne technologie, by chronić infrastrukturę krytyczną

Network & Information Security 2

Przeciwdziałanie incydentom

Artykuł 21, pkt 1

- Wprowadzenie **odpowiednich i proporcjonalnych środków technicznych**, operacyjnych i organizacyjnych
  w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych
- Proporcjonalność zastosowanych środków powinna zostać oceniona przy uwzględnieniu:
  - stopnia narażenia podmiotu na ryzyko,
  - wielkości podmiotu,
  - prawdopodobieństwa wystąpienia incydentu
  - dotkliwości potencjalnego incydentu, a w tym skutków społecznych i gospodarczych
- Obszary, w których należy zastosować środki zostały wskazane w **Artykule 21, pkt.2**

Jak dobrać nowoczesne technologie, by chronić infrastrukturę krytyczną

Network & Information Security 2

Przeciwdziałanie incydentom

Artykuł 21, pkt 2

- polityka analizy ryzyka i bezpieczeństwa systemów informatycznych;
- obsługa incydentu;
- **ciągłość działania**, np. zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej, i **zarządzanie kryzysowe**;
- bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami;
- bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie;
- polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie;
- **podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa**
- polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania;
- bezpieczeństwo zasobów ludzkich, politykę kontroli dostępu i zarządzanie aktywami;
- w stosownych przypadkach – **stosowanie uwierzytelniania wieloskładnikowego lub ciągłego**, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych.

Jakie procedury zwiększają bezpieczeństwo systemów OT

1. Segmentacja sieci
2. Zarządzanie dostępem
3. Zabezpieczenie punktów końcowych i urządzeń przemysłowych
4. Zarządzanie aktualizacjami i poprawkami
5. Monitorowanie i detekcja zagrożeń
6. Testy bezpieczeństwa i analiza ryzyka
7. Plany reagowania na incydenty
8. Szkolenie personelu OT
9. Zarządzanie cyklem życia urządzeń OT
10. Kontrola fizycznego dostępu

Jak skutecznie łączyć narzędzia i zasady w spójną strategię ochrony

🔧 **1. Zacznij od podstaw – stworzenie fundamentu strategii**

🧠 **2. Strategiczne połączenie zasad z technologią**

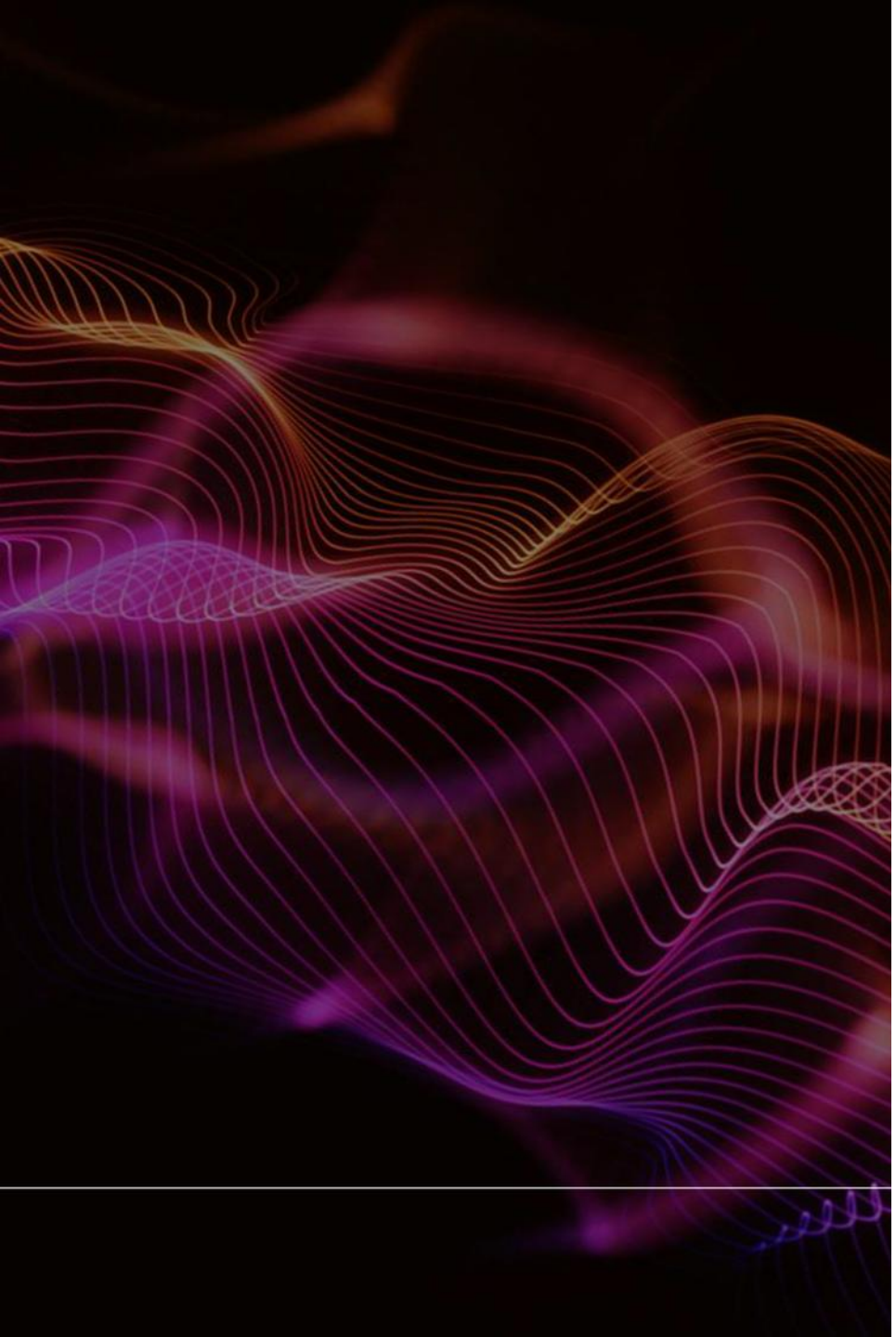
🧩 **3. Integracja technologii w jednej architekturze bezpieczeństwa**

👥 **4. Równoległe zabezpieczenie ludzi i procesów**

🔁 **5. Ciągłe doskonalenie i testowanie**

📊 **6. Dokumentacja i mierzenie skuteczności**

✅ PODSUMOWANIE STRATEGII:
🔄 **Polityki → narzędzia → procesy → ludzie → monitorowanie → korekty**



Dziękuję za uwagę

Damian Gołuch

damian.goluch@bakotech.com

bako tech®