Webinar
AI
w cyberbezpieczeństwie
Ryzyka i zagrożenia

The better the question. The better the answer. The better the world works.

Shape the future
with confidence

Marcin Nowicki
IT-Training & Consulting

Wykształcenie: Studia informatyczne na Technische Universität Darmstadt (Politechnika w Darmstadt)
Języki: polski, niemiecki, angielski

Doświadczenie zawodowe:

- Trener, wykładowca, doradca i coach
- Szkolenia z zakresu M365, baz danych i narzędzi do analizy danych, programowania, systemów operacyjnych, sztucznej inteligencji, bezpieczeństwa IT i wielu innych
- Projektowanie i programowanie baz danych oraz aplikacji
- Automatyzacja procesów
- Obsługa i administracja infrastruktury IT dla małych i średnich przedsiębiorstw
- Doradztwo przy wdrażaniu rozwiązań chmurowych M365 i Copilot w środowisku koncernowym

Kompetencje branżowe:

- Doświadczenie obejmuje bankowość, przemysł, motoryzację, sektor usług, doradztwo, IT oraz branże wysokich technologii (lotnictwo, kosmonautyka)
- Dostawcy usług IT, firmy szkoleniowe
- Ministerstwa, urzędy oraz inne instytucje państwowe
- Organizacje międzynarodowe i globalne (np. Europejski Bank Centralny oraz Organizacja Narodów Zjednoczonych)
- Stowarzyszenia, związki zawodowe

Tematy specjalizacji:

- M365 Copilot dla użytkowników i zaawansowanych użytkowników
- Microsoft Power Plattform (np. Power BI, Power Automate)
- Programowanie (np. Office Scripts, SQL, XML, HTML/CSS, C++, C#, Java, JavaScript)
- Sieci komputerowe (np. podstawy sieci, TCP/IP)
- Cyberbezpieczeństwo, podstawy kryptografii
- Techniki prezentacji i wystąpień publicznych

Wybrane referencje:

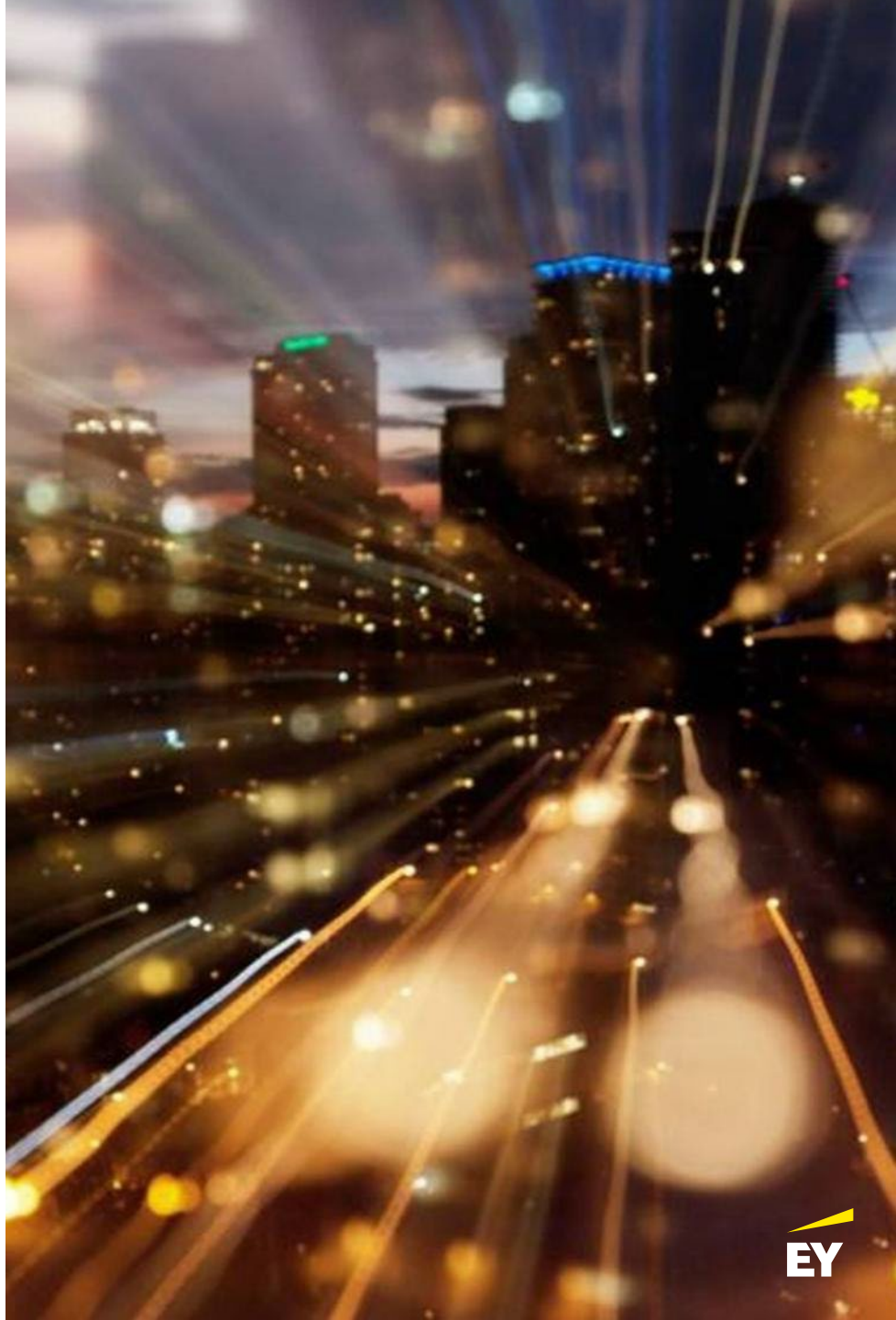
- Deutsche Bank, Credit Suisse, Crédit Agricole, PKO Bank Polski, BNP Paribas, Bank BPS, Deutsche Börse, Europejski Bank Centralny (ECB), Deutsche Bundesbank, Landesbank Hessen-Thüringen Girozentrale (Helaba), EY, PwC, Deloitte, Microsoft, SAP, Siemens, Airbus, Lufthansa, DHL, Orlen, RWE, IKEA, Lavazza, Uniwersytet w Heidelbergu
- Dodatkowe aktywności: Gospodarz audycji radiowej o tematyce IT, współorganizator międzynarodowych konferencji IT w Niemczech i USA

Doświadczenie projektowe:

- Prowadzenie szkoleń i treningów na całym świecie w języku niemieckim, angielskim i polskim, m.in. . w Polsce, Niemczech, Brazylii, Australii, Chinach, USA, RPA, Wielkiej Brytanii, Meksyku i wielu innych krajach
- Prywatny wykładowca na Uniwersytecie we Frankfurcie w zakresie informatyki, ze szczególnym uwzględnieniem bezpieczeństwa IT i ochrony danych
- Automatyzacja i optymalizacja procesów z wykorzystaniem Microsoft Power Platform oraz narzędzi sztucznej inteligencji dla średnich przedsiębiorstw i globalnych koncernów
- Projektowanie i rozwój oprogramowania, baz danych, szablonów i skryptów

Cyberataki w Polsce: realne ryzyko biznesowe

- +144,4% r/r (rekordowy wzrost)
- Polska w TOP 5 najbardziej atakowanych krajów UE
- 682 245 zgłoszeń incydentów
- Straty firm: 8% firm straciło >5 mln zł
- Cała gospodarka: ok. 2,8 mld zł strat rocznie
- AI przyspiesza i ułatwia przeprowadzanie ataków

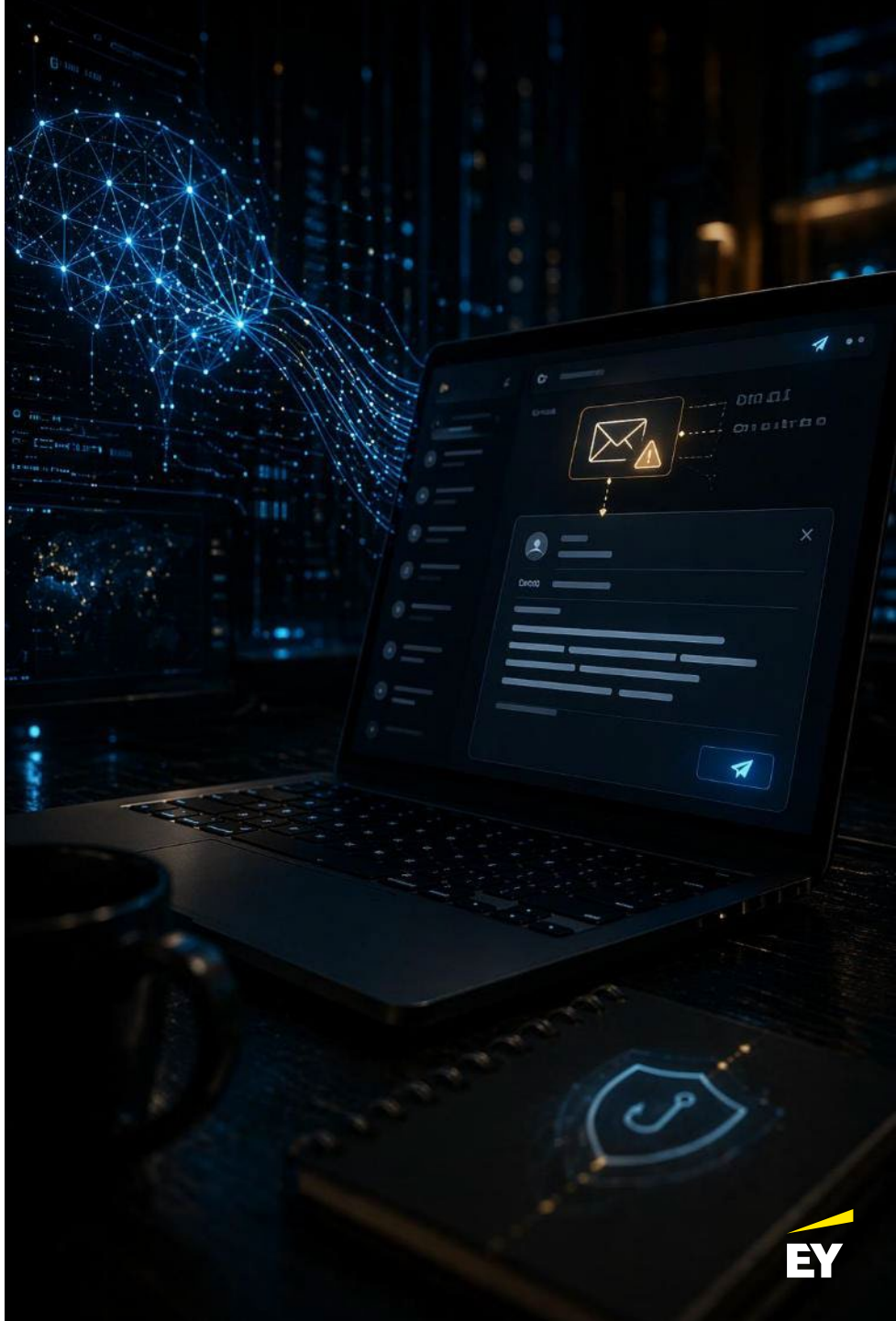


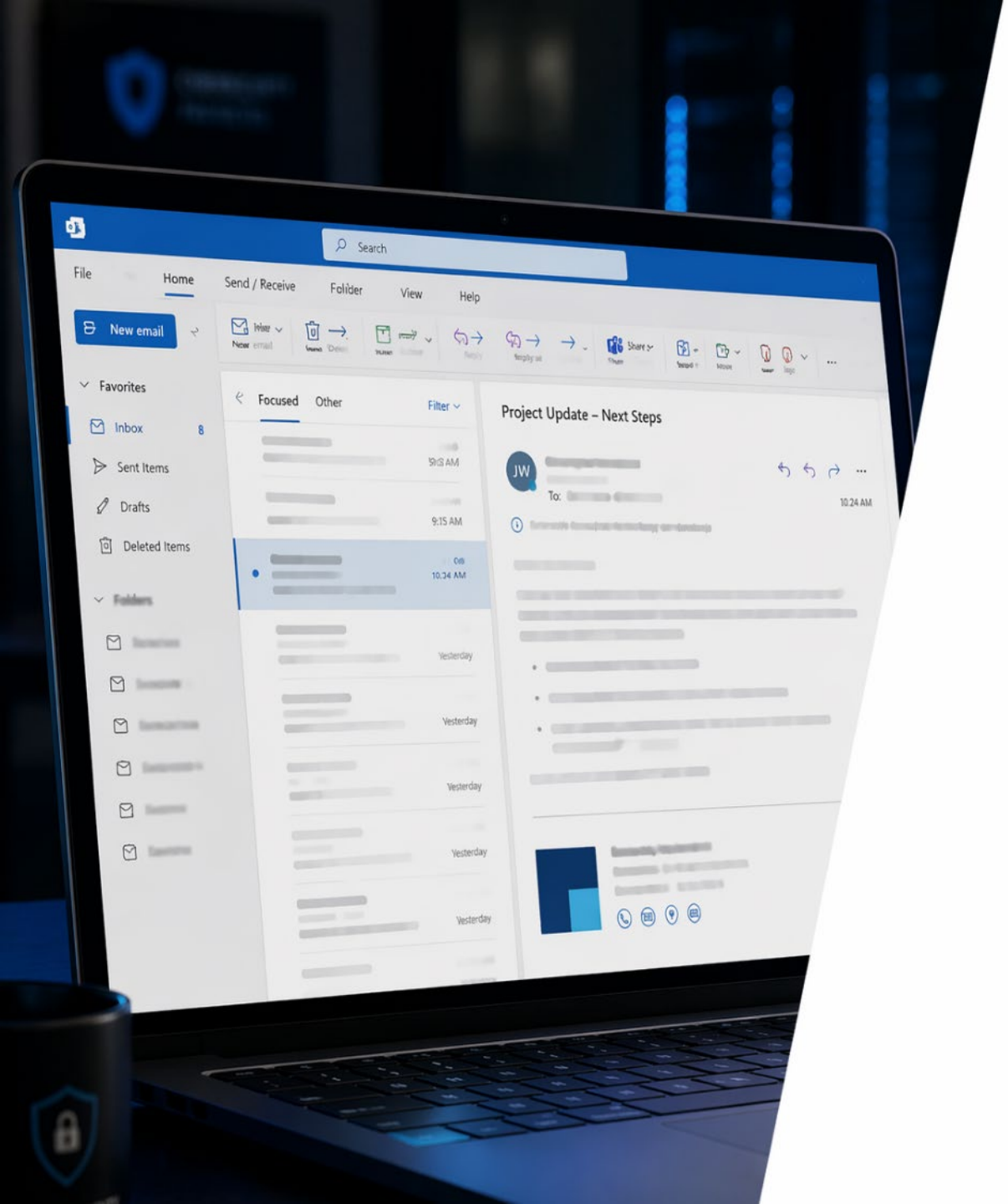
Rola AI w nowoczesnych cyberatakach

- Automatyczne tworzenie treści (e-maile, wiadomości, dokumenty)
- Analiza danych o ofiarze (lepsze dopasowanie ataku)
- Imitacja stylu komunikacji (np. przełożonego)
- Generowanie głosu i obrazu (deepfake)
- Automatyzacja ataków i łatwiejsze tworzenie exploitów
- Niższa bariera wejścia dla cyberprzestępców

Phishing w erze AI: co się zmieniło

- Brak błędów językowych i naturalny styl komunikacji
- Wiadomości dopasowane do osoby i kontekstu
- Podszywanie się pod przełożonych i współpracowników
- Wykorzystanie wielu kanałów (e-mail, Teams, SMS)
- Trudniejszy do wykrycia niż tradycyjny phishing





Przykład: wiadomość od „HR"

Od: Michał Nawrocki (HR)

Do: Marcin Nowicki

Temat: Aktualizacja danych pracowniczych

Dzień dobry,

w związku z aktualizacją systemu kadrowego prosimy o weryfikację i potwierdzenie danych pracowniczych. Proces jest obowiązkowy dla wszystkich pracowników i powinien zostać zakończony do końca dnia.

Formularz dostępny jest pod poniższym linkiem:
Aktualizacja danych

W przypadku pytań prosimy o kontakt.

Michał Nawrocki
Dział HR

Przykład: wiadomość na komunikatorze

Deepfake: gdy nie możesz ufać temu, co słyszysz i widzisz

- AI potrafi generować realistyczny głos i obraz
- Wystarczy kilka minut nagrania, aby odtworzyć czyjś głos (https://elevenlabs.io/)
- Możliwość podszywania się pod CEO lub przełożonego
- Wykorzystywane w atakach finansowych i socjotechnicznych
- Coraz trudniejsze do wykrycia

Deepfake Case: fałszywy telefon od „zarządu“

- Pracownik otrzymuje telefon od „CEO"
- Głos brzmi naturalnie i znajomo
- Polecenie: pilny przelew biznesowy
- Brak możliwości weryfikacji (presja czasu)
- Strata: setki tysięcy euro
- „Cześć, mam pilną sprawę. Potrzebny szybki przelew dla partnera dziś. Wyślę dane za chwilę. Dasz radę to ogarnąć w ciągu godziny?"

Ryzyka korzystania z AI w organizacji

- Błędne odpowiedzi i „halucynacje" AI
- Brak weryfikowalności źródeł
- Stronniczość modeli (bias)
- Ryzyko ujawnienia danych wrażliwych (shadow AI)
- Konsekwencje prawne i reputacyjne

Realne przypadki

Air Canada (2024)

- błędne informacje chatbotu → odpowiedzialność prawna
- Firma przegrywa sprawę i musi wypłacić odszkodowanie

Arup / Hong Kong (2024)

- deepfake CFO → strata ~25 mln USD
- Fałszywe spotkanie wideo z wykorzystaniem AI

AI w firmie: rosnące wymagania prawne

- UE wprowadza regulacje dotyczące AI (AI Act)
- Obowiązek kontrolowania ryzyk związanych z AI
- Odpowiedzialność za decyzje podejmowane przez AI
- Wymóg transparentności (np. chatboty, automatyczne decyzje)
- Firmy muszą wdrażać zasady korzystania z AI

Co to oznacza dla Twojej organizacji

- Cyberataki wykorzystujące AI będą się nasilać
- Największym celem jest człowiek, nie tylko system
- Tradycyjne metody wykrywania przestają działać
- Potrzebne są nowe zasady i świadomość pracowników
- Bezpieczeństwo to dziś proces, nie jednorazowe działanie