

Prezentacja „Ewolucja cyberprzestępczości w finansach” przedstawia rozwój zagrożeń w sektorze finansowym od pierwszych ataków do współczesnych wyzwań. Cyberprzestępczość, definiowana jako działania mające na celu kradzież danych lub pieniędzy, szczególnie dotyka instytucje finansowe z uwagi na ich zasoby i dane klientów. W latach 80. i 90. pojawiły się pierwsze wirusy komputerowe oraz oszustwa związane z kartami kredytowymi, a rozwój bankowości internetowej otworzył nowe możliwości dla przestępców. Wczesne ataki, takie jak phishing, były mniej zaawansowane, ale skuteczne ze względu na niską świadomość użytkowników. Współczesne zagrożenia obejmują phishing, ransomware oraz ataki DDoS, które znacząco zakłócają funkcjonowanie instytucji finansowych. Przykładem jest atak na JPMorgan Chase w 2014 roku, który dotknął 76 milionów klientów. Metody ataku ewoluowały wraz z rozwojem technologii – przestępcy wykorzystują sztuczną inteligencję, malware bezplikowy oraz urządzenia IoT do przeprowadzania bardziej zaawansowanych działań. Coraz częściej żądają okupów w kryptowalutach, co utrudnia ich śledzenie. Konsekwencje cyberataków dla sektora finansowego są ogromne – straty finansowe sięgają milionów dolarów, a reputacja instytucji ulega osłabieniu. Klienci tracą zaufanie do bankowości online i obawiają się o bezpieczeństwo swoich danych. W odpowiedzi sektor finansowy inwestuje w technologie ochronne, takie jak uwierzytelnianie wieloskładnikowe (MFA), szyfrowanie danych i architektura „Zero Trust”. Sztuczna inteligencja pomaga w wykrywaniu podejrzanych transakcji i blokowaniu zagrożeń w czasie rzeczywistym. Współpraca z regulatorami, takimi jak Unia Europejska (dyrektywa NIS2 i rozporządzenie DORA), odgrywa kluczową rolę w zwiększaniu bezpieczeństwa cyfrowego. Podsumowując, cyberprzestępczość stale ewoluuje wraz z technologią, wymuszając na sektorze finansowym ciągłe doskonalenie zabezpieczeń. Prognozy wskazują na wzrost liczby ataków wykorzystujących AI oraz kryptowaluty, co wymaga dalszych inwestycji w innowacyjne rozwiązania i międzynarodową współpracę.