mgr inż. Zofia Lubańska[1]
Akademia Bialska im. Jana Pawła II, Biała Podlaska

https://doi.org/10.29316/9788368103281_3

EWOLUCJA CYBERATAKÓW OD PHISHINGU DO RANSOMWARE-AS-A-SERVICE: MECHANIZMY, SKUTKI I STRATEGIE OBRONY

THE EVOLUTION OF CYBERATTACKS FROM PHISHING TO RANSOMWARE-AS-A-SERVICE: MECHANISMS, EFFECTS, AND DEFENSE STRATEGIES

Streszczenie

W niniejszym rozdziale dokonano przeglądu współczesnych cyberataków typu phishing i ransomware, ze szczególnym uwzględnieniem modelu Ransomware-as-a-Service (RaaS). Omówiono mechanizmy działania phishingu jako formy socjotechniki oraz ransomware – złośliwego oprogramowania szyfrującego dane i wymuszającego okup – a także ich ewolucję na przestrzeni ostatnich dekad. Przeanalizowano skalę zjawiska (częstość ataków i straty finansowe) oraz skutki społeczne i gospodarcze tych zagrożeń, w tym incydenty wpływające na infrastrukturę krytyczną i bezpieczeństwo ludzi. Rozdział przedstawia również rozwój modelu RaaS, który obniżył próg wejścia dla cyberprzestępców i przyczynił się do profesjonalizacji ataków ransomware. W części dyskusyjnej omówiono strategie obrony i środki zapobiegania tym atakom – od edukacji użytkowników po zaawansowane rozwiązania techniczne – oraz zarysowano przyszłe trendy, takie jak wykorzystanie sztucznej inteligencji zarówno przez atakujących (np. generowanie

[1] e-mail: z.lubanska@dyd.akademiabialska.pl.

przekonujących phishingów), jak i obrońców. Całość stanowi przegląd aktualnej wiedzy poparty literaturą przedmiotu, mający na celu wsparcie dalszych badań oraz praktycznych działań w zakresie cyberbezpieczeństwa.

Słowa kluczowe: phishing, ransomware, Ransomware-as-a-Service, cyberbezpieczeństwo, socjotechnika, cyberatak, obrona przed cyberatakami

Abstract

This article reviews contemporary phishing and ransomware cyberattacks, with particular emphasis on the Ransomware-as-a-Service (RaaS) model. It discusses the mechanisms of phishing as a form of social engineering and ransomware – malicious software that encrypts data and demands a ransom – as well as their evolution over the last few decades. The scale of the phenomenon (frequency of attacks and financial losses) and the social and economic impact of these threats, including incidents affecting critical infrastructure and human safety, are analysed. The chapter also presents the development of the RaaS model, which has lowered the entry threshold for cybercriminals and contributed to the professionalisation of ransomware attacks. The discussion section covers defence strategies and measures to prevent these attacks – from user education to advanced technical solutions – and outlines future trends, such as the use of artificial intelligence by both attackers (e.g., generating convincing phishing emails) and defenders. The work provides an overview of current knowledge, supported by literature on the subject, aimed at informing further research and practical activities in the field of cybersecurity.

Keywords: phishing, ransomware, Ransomware-as-a-Service, cybersecurity, social engineering, cyberattack, cyberattack defence

Wstęp

W dobie powszechnej cyfryzacji działalności prywatnej i zawodowej cyberzagrożenia stały się palącym problemem globalnym. Incydenty takie jak kradzieże danych, oszustwa internetowe czy ataki z użyciem złośliwego oprogramowania odnotowują lawinowy wzrost. Według raportów FBI Internet Crime Complaint Center w 2022 roku zgłoszono w USA ponad 800 tysięcy cyberprzestępstw, które spowodowały łączne straty przekraczające 10,2 mld USD (Lopez-Aguilar i in., 2025). Rok później liczba zgłoszeń osiągnęła rekordowe 880 tysięcy, a szkody finansowe oszacowano na ponad 12,5 mld USD (Lopez-Aguilar i in., 2025). Są to wartości dramatycznie wyższe niż jeszcze kilka lat temu, co pokazuje, że skala cyberzagrożeń dynamicznie rośnie.

Wśród rozmaitych form ataków, szczególną powszechnością odznacza się phishing. Szacuje się, że ataki phishingowe stanowią najczęstszy wektor naruszeń bezpieczeństwa – np. w 2023 roku aż 36% wszystkich wycieków danych było zapoczątkowanych atakiem phishingowym (Lopez-Aguilar i in., 2025). Ten typ ataku wykorzystuje czynnik ludzki: podatność użytkowników na manipulację i błędy. Nic dziwnego, skoro około 85% wszystkich incydentów naruszenia bezpieczeństwa wynika w pewnym stopniu z błędów człowieka (Lopez-Aguilar i in., 2025). Cyberprzestępcy celują więc w najsłabsze ogniwo systemu, stosując socjotechnikę zamiast łamania zabezpieczeń technicznych. Phishing – w najbardziej klasycznej formie – polega na wysyłaniu spreparowanych wiadomości (np. e-maili) imitujących zaufane instytucje, celem nakłonienia ofiary do podania danych wrażliwych lub zainfekowania jej urządzenia. Rozmiary tego zjawiska są ogromne: według Anti-Phishing Working Group w pierwszej połowie 2023 r. odnotowano 1,2 miliona ataków phishingowych na świecie, co stanowi wzrost o 40% względem roku poprzedniego (Lopez-Aguilar i in., 2025). Jednocześnie coraz częstsze są ataki złośliwym oprogramowaniem ransomware, które przynoszą wyjątkowo dotkliwe straty finansowe i operacyjne dla zaatakowanych firm czy instytucji. Ransomware polega na zaszyfrowaniu danych ofiary i żądaniu okupu za ich odszyfrowanie – jest to zatem cyfrowa forma wymuszenia (cybernetyczny odpowiednik „porwania" danych). Choć samych incydentów ransomware jest liczbowo mniej niż phishingów, to konsekwencje pojedynczego ataku ransomware bywają katastrofalne. W 2020 r. globalne szkody wyrządzone przez ransomware szacowano na 20 mld USD, podczas gdy jeszcze w 2019 r. było to ok. 11,5 mld (Meland i in., 2020). Prognozy wskazują dalszy gwałtowny wzrost – według analityków do 2025 r. roczne straty spowodowane atakami ransomware mogą sięgnąć 57 mld USD, a do 2031 r. nawet ćwierć biliona USD (Meland i in., 2020).

Phishing i ransomware często są ze sobą powiązane: phishing stał się głównym wektorem wprowadzającym ataki ransomware. Innymi słowy, wiele kampanii ransomware rozpoczyna się od pozornie niewinnej wiadomości phishingowej, zawierającej złośliwy załącznik lub link (Meland i in., 2020). Brak ostrożności użytkownika – jedno nieuważne kliknięcie – może zainicjować łańcuch zdarzeń prowadzących do szyfrowania całej sieci firmowej

przez ransomware. Takie wieloetapowe ataki pokazały swoją skuteczność m.in. podczas globalnej kampanii ransomware WannaCry w 2017 r., kiedy to wykorzystano prosty błąd użytkownika i zaniedbania aktualizacji systemu do infekcji setek tysięcy komputerów na świecie.

Celem niniejszej pracy jest przedstawienie w układzie przeglądowym ewolucji oraz charakterystyki dwóch wspomnianych klas ataków – phishingu i ransomware – a także modelu Ransomware-as-a-Service, który stanowi stosunkowo nowe zjawisko polegające na udostępnianiu ransomware w formie usługi. Zaprezentowano mechanizmy działania tych ataków, ich społeczne i ekonomiczne konsekwencje, oraz omówiono dostępne strategie obrony. Rozdział opiera się na aktualnej literaturze naukowej (analizie kilkunastu najnowszych prac z lat 2020-2025) oraz udokumentowanych przypadkach incydentów.

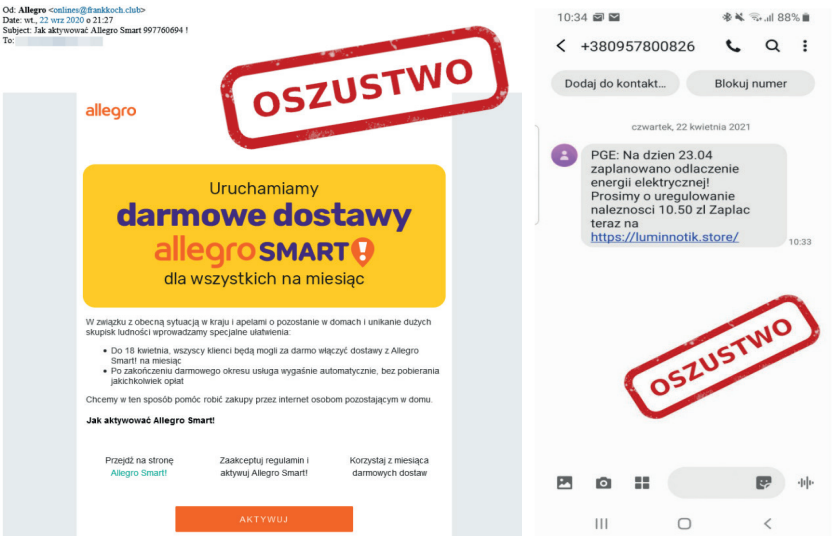
Metody

Praca ma charakter przeglądu literatury (narrative review). W celu zebrania informacji przeanalizowano publikacje naukowe dotyczące phishingu i ransomware, ze szczególnym uwzględnieniem danych o skali zjawiska, technik ataków, trendów ewolucyjnych oraz metod przeciwdziałania. Materiał źródłowy obejmował 10 wyselekcjonowanych publikacji z lat 2020-2025 o tematyce zgodnej z zakresem (m.in. przeglądy systematyczne, analizy trendów, badania nad RaaS), a także raporty instytucji branżowych (np. Verizon DBIR, raporty FBI IC3) oraz studia przypadków głośnych cyberataków. Kryteriami doboru literatury była aktualność (priorytet dla badań z ostatnich ~5 lat) oraz wysoka relewancja (publikacje skupione na phishingu, ransomware lub aspektach socjotechniki i RaaS). Przegląd obejmował zarówno prace o charakterze empirycznym (np. analizy danych incydentów), jak i artykuły przeglądowe oraz komentarze eksperckie, co pozwoliło na wieloaspektowe ujęcie tematu. Zebrane informacje usystematyzowano według schematu IMRaD – w części wynikowej przedstawiono kluczowe ustalenia dotyczące mechanizmów ataku, ich skutków oraz ewolucji, zaś w dyskusji omówiono implikacje praktyczne, środki zaradcze i kierunki dalszego rozwoju sytuacji.

Wyniki

Ataki phishingowe – mechanizmy i charakterystyka

Termin phishing wywodzi się od angielskiego *fishing* (wędkowanie) i trafnie oddaje istotę ataku: oszust „zarzuca przynętę" w postaci wiarygodnie wyglądającej wiadomości (e-mail, SMS itp.) i liczy, że ofiara „złapie haczyk". Phishing (rysunek 1) jest klasycznym przykładem ataku socjotechnicznego – wykorzystuje manipulację użytkownikiem zamiast zaawansowanych metod technicznych. Typowy scenariusz wygląda następująco: ofiara otrzymuje wiadomość pozornie pochodzącą od zaufanej instytucji (np. banku, operatora płatności, serwisu społecznościowego). Wiadomość często zawiera prośbę o pilne podjęcie działania – np. *„Twoje konto zostanie zablokowane, jeśli nie zweryfikujesz danych"* – i link prowadzący do strony imitującej prawdziwą witrynę. Nieświadoma podstępu ofiara wprowadza tam swoje hasło lub inne dane, które trafiają prosto do przestępców. Inną odmianą jest skłonienie do pobrania załącznika (np. rzekomej faktury), który zawiera złośliwy kod infekujący system ofiary.



Rysunek 1. Przykłady phishingu
Źródło: CERT Polska.

Phishing bazuje na wykorzystaniu ludzkich emocji i odruchów. Atakujący często stosują język wzbudzający strach lub presję czasu, aby uniemożliwić racjonalną ocenę sytuacji (Lopez-Aguilar i in., 2025). Przykładowo, e-mail grożący natychmiastowym zamknięciem konta bankowego wywołuje panikę i skłania do pochopnego kliknięcia w link. Inną techniką jest obiecywanie korzyści (np. wygranej w konkursie) – żądza zysku lub ciekawość mogą uśpić czujność ofiary. Ważną cechą phishingu jest także wiarygodność pozorów: wiadomości bywają dopracowane graficznie i językowo, zawierają autentycznie wyglądające logotypy i dane instytucji. Mimo to często można dostrzec pewne sygnały ostrzegawcze. Należą do nich np. drobne błędy w tekście czy adresie nadawcy – oszuści rejestrują domeny internetowe łudząco podobne do prawdziwych (np. paypal.com vs paypa1.com z cyfrą „1" zamiast litery „l"), licząc, że użytkownik nie zauważy różnicy (Lopez-Aguilar i in., 2025). Uwagę powinny zwrócić także nietypowe prośby w wiadomości: żaden prawdziwy bank lub urzędnik nie wymaga podania całego hasła czy kodu PIN przez e-mail. Phisherzy chętnie wykorzystują również nowe kanały komunikacji – poza e-mailami spotyka się SMS-phishing (smishing), a nawet próby telefoniczne, czyli voice phishing (vishing), gdzie oszust podszywa się pod pracownika instytucji.

Pomimo istnienia tych potencjalnych sygnałów ostrzegawczych phishing pozostaje niezwykle skuteczny. Dzieje się tak z kilku powodów związanych z czynnikiem ludzkim. Po pierwsze, braki świadomości i wiedzy – wiele osób nigdy nie przeszło szkolenia z cyberbezpieczeństwa i nie potrafi rozpoznać nawet podstawowych oznak oszustwa. Po drugie, rutyna i pośpiech – w natłoku codziennej korespondencji użytkownicy często działają mechanicznie, nie weryfikując nadawców ani treści komunikatów. Przestępcy świadomie tworzą sytuację presji czasu lub wyjątkowości („ostateczne ostrzeżenie", „niepowtarzalna okazja"), by skłonić ofiarę do działania przed myśleniem. Po trzecie, aspekt psychologiczny – nawet osoby ostrożne mogą ulec dobrze zaprojektowanej manipulacji, zwłaszcza gdy wiadomość budzi silne emocje (strach, ciekawość, chęć pomocy bliskiemu w potrzebie itp.). Statystyki wskazują, że czynnik ludzki odgrywa rolę w ogromnej większości naruszeń bezpieczeństwa – jak wspomniano, aż ~85% incydentów jest wynikiem błędów po stronie użytkowników (Lopez-Aguilar i in., 2025). To

tłumaczy, dlaczego phishing tak bardzo upodobał sobie atakowanie ludzkiej podatności, zamiast prób obejścia technicznych zabezpieczeń.

Co ważne, phishing często nie jest celem samym w sobie, lecz środkiem do osiągnięcia kolejnych etapów ataku. Uzyskanie danych uwierzytelniających ofiary może posłużyć np. do zalogowania się na jej konto pocztowe lub firmowe, skąd atakujący rozszerzy dostęp do kolejnych zasobów. W kontekście niniejszego rozdziału kluczowe jest, że phishing stał się główną metodą dostarczania złośliwego oprogramowania ransomware do sieci ofiar (Meland i in., 2020). Przykładowy scenariusz: pracownik firmy otrzymuje e-mail podszywający się pod dział IT z prośbą o pilną „aktualizację hasła" – po kliknięciu w link i wprowadzeniu danych napastnik zdobywa jego poświadczenia. Następnie wykorzystuje je, by zalogować się do sieci firmowej i tam umieszcza ransomware, który po pewnym czasie szyfruje dane całej organizacji. W ten sposób jedno nieostrożne kliknięcie uruchamia lawinę skutków.

Skala zagrożenia phishingiem jest ogromna. Badania i statystyki zgodnie wskazują phishing jako najczęstszą formę ataku cybernetycznego na świecie. Przykładowo, w reprezentatywnym badaniu firm brytyjskich w 2025 r. aż 37% wszystkich przedsiębiorstw doświadczyło w minionym roku choćby jednej udanej próby phishingu, co czyniło go najpowszechniejszym typem incydentu (wśród firm dotkniętych jakimkolwiek naruszeniem bezpieczeństwa phishing stanowił 85% przypadków) (GOV.UK, 2025). Dla porównania, znacznie rzadsze były inne rodzaje ataków – np. bezpośrednie infekcje ransomware zgłosiło tylko ~3% firm (co odpowiada 7% przypadków wśród firm dotkniętych cyberprzestępczością) (GOV.UK, 2025). Dane te pokazują, że phishing jest wszechobecny i stanowi podstawowe narzędzie w arsenale cyberprzestępców.

Ataki ransomware – działanie i ewolucja zagrożenia

Ransomware uznawany jest za jedno z najgroźniejszych współczesnych zagrożeń cybernetycznych. Działanie ransomware można przyrównać do sytuacji, gdy ktoś zakłada kłódkę na drzwi naszego domu i żąda okupu za klucz. Po udanym ataku ransomware pliki na zaatakowanym komputerze lub sieci zostają zaszyfrowane za pomocą silnej kryptografii (np. algorytmów

AES/RSA) – stają się nieczytelne bez unikalnego klucza deszyfrującego, który posiadają napastnicy. Ofiara otrzymuje informację (notatkę okupu), że aby odzyskać dostęp do swoich danych, musi zapłacić określoną sumę – zazwyczaj w kryptowalucie, najczęściej Bitcoinach, co zapewnia przestępcom anonimowość transakcji (Meland i in., 2020). Staje wobec dramatycznego dylematu: zapłacić okup (licząc na obietnicę odszyfrowania, choć gwarancji nie ma) czy pogodzić się z utratą danych. Coraz częściej atakujący stosują tzw. podwójne wymuszenie: przed zaszyfrowaniem kradną część danych i grożą ich publikacją, jeśli okup nie zostanie wpłacony (Meland i in., 2020). Ma to dodatkowo zmotywować ofiarę (zwłaszcza firmę) do zapłaty z obawy przed wyciekiem wrażliwych informacji.

Typowy przebieg ataku ransomware obejmuje kilka faz. Faza infekcji: przestępcy muszą znaleźć sposób na uruchomienie złośliwego programu (ransomware) w środowisku ofiary. Najczęściej odbywa się to poprzez socjotechnikę – np. otwarcie przez ofiarę zainfekowanego załącznika (dokumentu MS Office z makrem, pliku PDF, fałszywej aplikacji) lub kliknięcie linku pobierającego malware. Inną metodą jest wykorzystanie luki w oprogramowaniu (tzw. exploit) – np. nierzadko ransomware rozprzestrzenia się automatycznie poprzez znane podatności systemu operacyjnego, co było przypadkiem wspomnianego WannaCry w 2017 r. Po zainstalowaniu w systemie, złośliwe oprogramowanie często rozprzestrzenia się dalej – jeśli atak dotyczy sieci firmowej, ransomware stara się zainfekować jak najwięcej urządzeń (komputerów, serwerów) w celu zmaksymalizowania szkód (Meland i in., 2020). Następnie następuje faza szyfrowania danych: malware aktywuje moduł szyfrujący, który przekształca pliki (dokumenty, bazy danych, zdjęcia itp.) w zaszyfrowaną postać. Często rozszerzenia plików zostają zmienione na specyficzne (np. locked, crypt), by ofiara zauważyła, że coś jest nie tak (Meland i in., 2020). Gdy proces szyfrowania się zakończy, ransomware wyświetla komunikat z żądaniem okupu – np. w postaci pliku tekstowego umieszczonego na pulpicie lub okna aplikacji. W notatce napastnicy informują, co się stało (zaszyfrowanie danych) oraz podają instrukcje zapłaty okupu (np. adres portfela Bitcoin i termin płatności, po którym cena wzrośnie lub klucz zostanie zniszczony) (Meland i in., 2020). Często grożą też, że próby samodzielnego usunięcia wirusa lub odszyfrowania danych spowodują trwałe uszkodzenie plików. W ten sposób

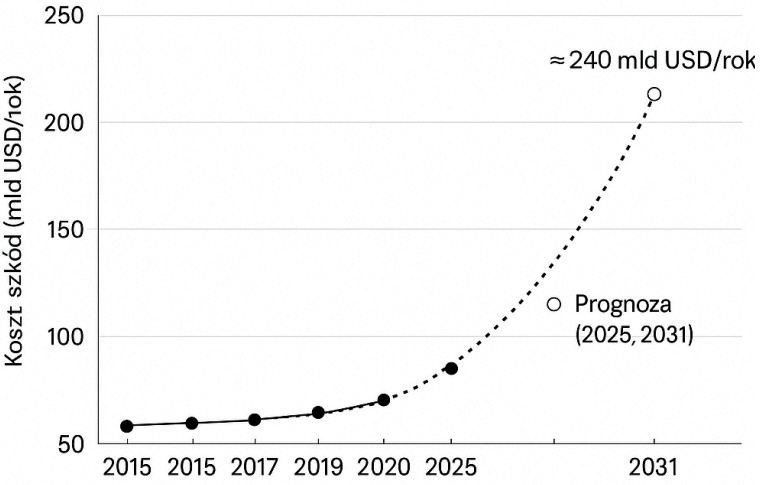
ofiara jest poddana maksymalnej presji psychologicznej. Wielu ekspertów bezpieczeństwa stanowczo odradza płacenie okupu – po pierwsze dlatego, że finansuje to dalszą działalność przestępców, po drugie zaś nie daje gwarancji odzyskania danych (napastnicy mogą nie dostarczyć klucza lub zażądać kolejnej zapłaty). Niemniej w sytuacji kryzysowej, zwłaszcza gdy stawką są krytyczne dane firmowe lub ludzkie życie (np. gdy celem jest szpital), presja na zapłacenie bywa ogromna (Meland i in., 2020).

Choć mogłoby się wydawać, że ransomware to nowy wynalazek XXI wieku, jego geneza sięga końca lat 80. XX w. Za pierwszy udokumentowany przypadek ataku ransomware uznaje się tzw. AIDS Trojan (PC Cyborg) z 1989 roku. W ramach tego incydentu rozesłano pocztą tradycyjną dyskietki z pozornie naukowym programem dotyczącym AIDS; po kilkudziesięciu uruchomieniach program szyfrował nazwy plików na komputerze i żądał okupu w wysokości 189 dolarów, wysyłanych przekazem pocztowym na wskazany adres w Panamie (Meland i in., 2020). Atak ten, choć ciekawy z historycznego punktu widzenia, był odosobniony i relatywnie prymitywny – szyfrowanie danych dało się dość łatwo odwrócić przez specjalistów, a technika nie znalazła naśladowców przez kolejne lata. Dopiero po ponad dwóch dekadach nastąpił prawdziwy rozkwit ransomware. Około roku 2013-2014 zauważalna jest eksplozja liczby nowych rodzin ransomware (np. CryptoLocker, który pojawił się w 2013 r., jest często wskazywany jako punkt zwrotny) (Meland i in., 2020). Zbiegło się to w czasie z upowszechnieniem kryptowaluty Bitcoin, która ułatwiła atakującym anonimowe pobieranie okupów, oraz ogólnym wzrostem cyfryzacji danych w społeczeństwie (co uczyniło wymuszanie okupów bardziej opłacalnym). W połowie lat 2010. mieliśmy do czynienia z „boomem" ransomware – powstały dziesiątki nowych odmian i odnotowywano tysiące infekcji na całym świecie. Początkowo ofiarami byli głównie użytkownicy indywidualni, lecz z czasem przestępcy zorientowali się, że znacznie większe zyski osiągną, atakując przedsiębiorstwa i instytucje publiczne.

Przełomowym zjawiskiem okazało się pojawienie modelu Ransomware-as-a-Service (RaaS). Około 2015 roku cyberprzestępcze podziemie zaczęło oferować gotowe pakiety ransomware na sprzedaż lub wynajem – czyli ransomware w modelu usługowym (Meland i in., 2020). Twórcy złośliwego oprogramowania zaczęli działać niczym dostawcy usług: przygotowują oni

kompletny „produkt" (kod ransomware, panel sterujący, instrukcje obsługi), który następnie udostępniają odpłatnie innym osobom (tzw. afiliantom). Afilianci płacą prowizję lub dzielą się zyskami z twórcami w zamian za możliwość wykorzystania ransomware na własnych celach. Model ten radykalnie obniżył barierę wejścia do świata ransomware – do przeprowadzania ataków nie jest już wymagana wysoka wiedza programistyczna ani zaplecze techniczne; wystarczy zakupić usługę na darknecie (Meland i in., 2020). RaaS zdemokratyzował więc cyberprzestępczość: nawet mniej zaawansowani technicznie przestępcy mogą obecnie wywołać poważne incydenty bezpieczeństwa (Meland i in., 2020). W efekcie nastąpił gwałtowny wzrost liczby grup ransomware operujących globalnie. Szacuje się, że większość aktywnych w ostatnich latach grup (takich jak REvil, DarkSide, LockBit i wiele innych) działa w modelu RaaS lub zbliżonym. Zjawisku temu towarzyszy profesjonalizacja działalności przestępczej – gangi ransomware funkcjonują coraz bardziej jak przedsiębiorstwa (posiadają strukturę podziału zadań, „działy wsparcia klienta", systemy reputacyjne na forach, a nawet programy partnerskie) (Fisher i in., 2025; Botchkovar i in., 2025). Niestety, implikuje to również coraz większą skuteczność i zuchwałość ataków ransomware. O ile dawniej typowy okup wynosił równowartość kilkuset dolarów (atakujący celowali w przeciętnych użytkowników), o tyle obecnie standardem stają się żądania rzędu setek tysięcy lub milionów dolarów od zaatakowanych przedsiębiorstw. Odnotowano przypadki, gdy przestępcy początkowo żądali od ofiary okupu 50-60 mln USD, by ostatecznie „zgodzić się" na negocjacjach na nieco niższą kwotę – np. w ataku na amerykańską firmę ubezpieczeniową CNA Financial w 2021 r. okup zredukowano z 60 mln do 40 mln USD (Zhang, Luo, 2025). Równie wysokich sum (rzędu kilkudziesięciu milionów dolarów) domagały się gangi w innych głośnych incydentach, co jeszcze kilka lat temu wydawało się nieprawdopodobne. Obecnie jednak okupy liczone w dziesiątkach milionów USD nie należą do rzadkości.

Powyższe czynniki sprawiły, że ransomware przeobraziło się w ostatnich latach w globalny multimilionowy biznes przestępczy. Szacuje się, że w 2021 r. światowe koszty spowodowane atakami ransomware wyniosły ok. 20 mld USD, a do 2031 r. mogą wzrosnąć nawet do 240 mld USD rocznie (Meland i in., 2020). Poniższy wykres ilustruje tę dynamikę wzrostu.



Rysunek 2. Wzrost globalnych kosztów szkód wyrządzanych przez ransomware w latach 2015-2031
Źródło: Meland i in., 2020.

Punkty oznaczają wartości szacowane historyczne (2015-2021) oraz prognozy analityków na 2025 i 2031 rok. Zauważalny jest wykładniczy trend wzrostowy – prognoza na 2031 r. (ok. 240 mld USD rocznie) oznacza, że koszty te byłyby ponad 20-krotnie większe niż w roku 2021.

Skutki społeczne i gospodarcze cyberataków

Rosnąca skala ataków phishingowych i ransomware przekłada się na wymierne konsekwencje dla społeczeństwa i gospodarki. W odróżnieniu od wielu tradycyjnych przestępstw, cyberataki uderzają nie tylko w systemy komputerowe, ale pośrednio w realne procesy życiowe ludzi i funkcjonowanie instytucji.

Ataki ransomware na infrastrukturę krytyczną stanowią szczególne zagrożenie. Głośnym przykładem był incydent z maja 2021 r., gdy ransomware zaatakował sieć firmową operatora rurociągu paliwowego Colonial Pipeline w USA. W obliczu paraliżu systemów, firma prewencyjnie wstrzymała działanie rurociągu zaopatrującego w benzynę całe wschodnie wybrzeże USA, co spowodowało kilkudniowe braki paliwa na stacjach i panikę wśród kierowców (Botchkovar i in., 2025). Operator zdecydował się ostatecznie zapłacić

okup (4,4 mln USD w Bitcoin) dla przywrócenia działania, co unaoczniło, że skutki ataku cyfrowego mogą rozlać się szeroko na gospodarkę kraju. Innym drastycznym przykładem jest atak ransomware na szpital uniwersytecki w Düsseldorfie we wrześniu 2020 r. – wskutek zaszyfrowania systemów szpital musiał przekierować karetkę z ciężko chorą pacjentką do odleglejszej placówki, co opóźniło zabieg o godzinę; pacjentka niestety zmarła, a prokuratura niemiecka wszczęła postępowanie, uznając, że atak mógł przyczynić się do tej śmierci (Alder, 2020). Są to prawdopodobnie pierwsze udokumentowane sytuacje, gdzie cyberatak ransomware doprowadził pośrednio do zagrożenia życia lub utraty życia ludzkiego.

Nawet jeśli nie dochodzi do tak tragicznych skutków, straty finansowe i operacyjne spowodowane ransomware dla zaatakowanych organizacji są ogromne. Poza kosztem ewentualnego okupu (który nierzadko sięga milionów), firmy ponoszą wydatki na przywracanie systemów do działania, wymianę sprzętu, audyty bezpieczeństwa, poprawę zabezpieczeń po incydencie, a często również muszą wypłacać odszkodowania lub pokrywać kary (np. za wyciek danych osobowych klientów, co podlega karom na mocy przepisów o ochronie danych, takich jak RODO). Do tego dochodzą straty mniej policzalne: przestoje w działalności (np. fabryki czy porty tracące produkcję przez paraliż systemów IT), utrata zaufania klientów i reputacji marki, której dane zostały naruszone, a w skrajnych przypadkach utrata przewagi konkurencyjnej (gdy wyciekają poufne projekty, patenty itp.). Dla dużych korporacji atak ransomware to koszt liczony często w dziesiątkach milionów dolarów i zakłócenia ciągnące się miesiącami. Dla małych i średnich firm może to być cios śmiertelny – szacunki wskazują, że znaczący odsetek MŚP, które padły ofiarą poważnego ataku ransomware, nie wraca już do działalności i w ciągu roku ogłasza upadłość z powodu strat (GOV.UK, 2025).

Konsekwencje ataków phishingowych mają nieco inny charakter, choć również są dotkliwe. Phishing często uderza w osoby prywatne, które tracą oszczędności życia przelane na konta oszustów podszywających się np. pod policję czy bank (np. popularny w Polsce scam „na policjanta CBŚP"). Poza wymierną stratą finansową ofiary przeżywają traumę psychologiczną – wstyd, złość na siebie, poczucie krzywdy. Badania dokumentują przypadki osób, które po padnięciu ofiarą oszustwa internetowego popadły w głęboką

depresję, a nawet targnęły się na swoje życie (Lopez-Aguilar i in., 2025). Utrata zaufania do bankowości elektronicznej czy generalnie do usług cyfrowych jest również istotnym społecznie skutkiem – każda głośna kampania phishingowa nadszarpuje pewność użytkowników co do bezpieczeństwa korzystania z sieci. W skali makro powtarzające się ataki podważają wiarygodność systemów cyfrowych i mogą hamować tempo transformacji cyfrowej w społeczeństwie (skoro ludzie boją się korzystać z e-administracji czy bankowości online, państwo i firmy ponoszą koszty alternatywne braku zaufania).

Podsumowując, zarówno phishing, jak i ransomware generują wielowymiarowe szkody: finansowe (utraty pieniędzy, koszty odtworzenia danych), operacyjne (przerwy w działaniu infrastruktury, konieczność reorganizacji pracy), prawne (odpowiedzialność za wycieki danych) oraz społeczne (poczucie zagrożenia, stres, utrata zaufania do cyfrowych usług). Co gorsza, te rodzaje ataków często się ze sobą łączą – udany phishing może prowadzić do infekcji ransomware, a skuteczny atak ransomware często poprzedzony jest rozpoznaniem socjotechnicznym.

Poniższa tabela syntetycznie porównuje kluczowe cechy ataków phishingowych i ransomware, a także modelu Ransomware-as-a-Service.

Tabela 1. Porównanie ataków phishingowych, ransomware oraz modelu Ransomware-as-a-Service pod kątem ich charakterystyki, wymagań i skutków

Cecha	**Phishing (socjotechnika)**	**Ransomware (atak malware)**	**Ransomware-as--a-Service (model usługowy)**
Wektor ataku	Fałszywe komunikaty (e-mail, SMS, telefon) skłaniające ofiarę do podania danych lub instalacji złośliwego pliku (Lopez-Aguilar i in., 2025).	Złośliwe oprogramowanie dostarczane zazwyczaj poprzez załącznik phishingowy lub exploit w systemie ofiary (Meland i in., 2020).	Udostępnianie ransomware na darknetowych forach i marketach; przestępcy kupują gotowy „produkt" do wykorzystania (Meland i in., 2020).

Cecha	Phishing (socjotechnika)	Ransomware (atak malware)	Ransomware-as--a-Service (model usługowy)
Wymagana wiedza atakującego	Niska – ataki może przeprowadzić pojedyncza osoba przy minimalnych umiejętnościach technicznych (ważniejsza jest znajomość socjotechniki).	Średnia/Wysoka – napisanie lub zmodyfikowanie ransomware wymaga zaawansowanych umiejętności programistycznych, choć użycie gotowego ransomware (np. Emotet, CobaltStrike) jest łatwiejsze.	Niska po stronie afilianta – twórcy RaaS zapewniają pełne zaplecze techniczne. RaaS obniża barierę wejścia: osoby o ograniczonej wiedzy mogą wywołać poważny atak, korzystając z narzędzi stworzonych przez innych (Meland i in., 2020).
Cel i skutek bezpośredni	Kradzież danych uwierzytelniających, numerów kart, wyłudzenie przelewu itp. Skutek: utrata informacji lub pieniędzy przez ofiarę, często otwarcie drogi do dalszych ataków (np. przejęcia konta).	Zaszyfrowanie danych ofiary i sparaliżowanie systemów. Skutek: wymuszenie – ofiara traci dostęp do swoich zasobów, działalność zostaje przerwana do czasu odszyfrowania (czyli zapłacenia okupu lub przywrócenia danych z kopii).	Model biznesowy ransomware: zwiększenie skali ataków i zysków. Skutek: profesjonalizacja cyberprzestępczości – więcej ataków ransomware na świecie, także wymierzonych w większe cele (organizacje), wskutek łatwiejszej dostępności narzędzi (Fisher i in., 2025; Botchkovar i in., 2025).
Typowe ofiary	Szerokie spektrum: od użytkowników indywidualnych po pracowników firm (phishing masowy) oraz osoby na stanowiskach (spear phishing, whaling). Często punkt wyjścia do ataku na organizację.	Coraz częściej duże organizacje: przedsiębiorstwa, szpitale, szkoły, urzędy, infrastruktury krytyczne. Zdarzają się też ataki na osoby prywatne, ale okup i szkody są wtedy mniejsze.	Ofiary końcowe jak w kolumnie obok (firmy, instytucje), jednak model RaaS potęguje zagrożenie – pozwala atakować wielu różnym grupom celom globalnie. RaaS sprawia, że nawet sektor MŚP czy administracja lokalna może stać się celem (afilianci wybierają cele dowolnie).

Cecha	Phishing (socjotechnika)	Ransomware (atak malware)	Ransomware-as--a-Service (model usługowy)
Częstotliwość/ incydenty	Bardzo wysokie – miliony prób dziennie globalnie. Phishing odpowiada za większość prób ataków cyber (np. ~90% naruszeń bezpieczeństwa inicjowanych jest phishingiem lub pokrewną socjotechniką) (Lopez-Aguilar i in., 2025).	Relatywnie niższa liczba incydentów, ale rośnie z każdym rokiem. Ransomware stanowi kilka-kilkanaście procent wszystkich cyberataków zgłaszanych oficjalnie, ale powoduje nieproporcjonalnie duże szkody finansowe (GOV.UK, 2025).	Trudna do oszacowania – oferta RaaS jest obecna na darknet (setki ogłoszeń), ale nie każde przeradza się w atak. Trend wskazuje na wzrost: co roku pojawiają się nowe grupy RaaS i ataki przez nie przeprowadzane. Model RaaS jest rosnącym segmentem „rynku" cyberprzestępczości (Meland i in., 2020).
Przykładowe głośne incydenty	2016: atak phishingowy na pracownika firmy wydobywczej Leoni – utrata €40 mln wskutek fałszywego e-maila od rzekomego dyrektora finansowego (tzw. scam BEC).		

Źródło: opracowanie własne.

Dyskusja

Strategie obrony i mechanizmy przeciwdziałania

Analizowane zagrożenia są poważne, jednak wiele incydentów można skutecznie powstrzymać poprzez zastosowanie podstawowych zasad bezpieczeństwa oraz dobrych praktyk zarówno technicznych, jak i organizacyjnych. Wyniki przeglądu literatury oraz rekomendacje ekspertów wskazują na potrzebę wieloaspektowej strategii obrony, łączącej działania technologiczne z edukacją użytkowników.

Po pierwsze, podniesienie świadomości i szkolenia użytkowników stanowią fundamentalną linię obrony przed phishingiem. Skoro czynnik ludzki

jest najsłabszym ogniwem (85% incydentów spowodowanych błędem człowieka (Lopez-Aguilar i in., 2025)), inwestycja w ludzi jest kluczowa. Organizacje powinny regularnie szkolić pracowników z rozpoznawania prób phishingu, np. poprzez organizowanie kampanii symulowanych ataków (kontrolowany phishing testowy). Badania pokazują, że nawet proste szkolenia potrafią znacząco zmniejszyć odsetek osób klikających w podejrzane linki (Lopez-Aguilar i in., 2025). Ważne jest również kształtowanie „kultury bezpieczeństwa" – zachęcanie do zgłaszania podejrzanych wiadomości, otwarta komunikacja o incydentach, przypominanie w organizacji, że czujność każdego pracownika przekłada się na bezpieczeństwo całości.

Po drugie, od strony technicznej istnieje szereg narzędzi wspierających ochronę. Filtry antyphishingowe w systemach pocztowych (wykorzystujące m.in. mechanizmy sztucznej inteligencji do analizy wiadomości) potrafią automatycznie odrzucić dużą część phishingowych e-maili zanim trafią one do skrzynek użytkowników (Malik i in., 2025; CECOM CIO G6 Cybersecurity, 2024). Nowoczesne systemy potrafią wykrywać charakterystyczne cechy ataków (np. masowe wysyłki z nowych domen, nietypowe wzorce językowe generowane przez AI itp.). Oprogramowanie antywirusowe i antymalware z aktualnymi bazami zagrożeń jest kolejną warstwą obrony – może zablokować znane złośliwe załączniki lub linki prowadzące do exploitów. Niezmiernie ważne są aktualizacje oprogramowania i łatanie podatności: wiele ataków ransomware (jak WannaCry) powiodło się tylko dlatego, że ofiary nie zainstalowały w porę poprawek bezpieczeństwa, mimo że istniały one na długo przed atakiem (CECOM CIO G6 Cybersecurity, 2024). Stosowanie zasady regularnych aktualizacji systemu operacyjnego, przeglądarek, pakietów biurowych itp. znacznie ogranicza ryzyko zainfekowania poprzez exploit.

Kluczowym mechanizmem ochrony przed skutkami ewentualnego ataku ransomware są kopie zapasowe (backupy). Utrzymywanie regularnych backupów krytycznych danych – i przechowywanie ich w odizolowany sposób (offline lub w bezpiecznej chmurze) – pozwala odtworzyć zasoby bez płacenia okupu w razie ich zaszyfrowania (CECOM CIO G6 Cybersecurity, 2024). Złotym standardem stała się zasada 3-2-1 (trzy kopie danych, na dwóch różnych nośnikach, z czego jedna przechowywana offline). Oczywiście, same kopie muszą być również zabezpieczone przed atakiem (np. odłączone od

sieci, by ransomware nie mógł ich zaszyfrować). Organizacje, które wdrożyły solidne strategie backupu i plan odtwarzania awaryjnego (disaster recovery), są w stanie względnie szybko podnieść się po ataku, unikając płacenia okupu.

Dodatkowe środki techniczne obejmują m.in.: uwierzytelnianie dwuskładnikowe (2FA) – nawet jeśli hasło użytkownika wycieknie w phishingu, to dodatkowy token (SMS, aplikacja) może powstrzymać napastnika przed zalogowaniem (CECOM CIO G6 Cybersecurity, 2024). Segmentacja sieci i ograniczanie uprawnień – dzięki podziałowi sieci firmowej na segmenty (strefy) ransomware nie rozprzestrzeni się automatycznie na wszystkie zasoby, a konta użytkowników z ograniczonymi uprawnieniami nie pozwolą mu od razu przejąć kontroli nad serwerami. Monitorowanie i detekcja anomalii – systemy klasy IDS/IPS oraz narzędzia SIEM z mechanizmami analizy behawioralnej mogą wykryć nietypowe działania wskazujące na atak (np. masowe szyfrowanie plików w sieci) i automatycznie zaalarmować administratorów lub nawet zablokować ruch. Coraz większe nadzieje wiąże się z zastosowaniem sztucznej inteligencji w obronie – algorytmy uczące się normalnego zachowania sieci mogą szybciej i skuteczniej identyfikować subtelne oznaki włamania lub phishingu, zanim człowiek zwróci na nie uwagę.

Mimo postępu technologicznego, w obronie przed phishingiem i ransomware wciąż niezastąpiony jest zdrowy rozsądek oraz czujność ludzka. To użytkownik na końcu podejmuje decyzję o kliknięciu linku czy otwarciu załącznika. Dlatego eksperci podkreślają, że skuteczna strategia musi być wielowarstwowa – łączenie świadomości i edukacji z narzędziami technicznymi daje najlepsze rezultaty (Malik i in., 2025; CECOM CIO G6 Cybersecurity, 2024). Przykładowo, szkolenia z phishingu są dużo bardziej efektywne, jeśli pracownicy wiedzą, że firmowa poczta i tak odfiltrowuje większość podejrzanych wiadomości – dzięki temu w skrzynce zostaje tylko niewielka liczba potencjalnie groźnych e-maili, którym mogą poświęcić więcej uwagi. Z kolei najlepszy system backupowy na nic się nie zda, jeśli personel zapomni go skonfigurować lub regularnie testować odtwarzania danych.

Nowe trendy i przyszłe wyzwania

Krajobraz zagrożeń cybernetycznych nieustannie ewoluuje – można go porównać do wyścigu zbrojeń między atakującymi a obrońcami. Na horyzoncie najbliższych lat wyłania się kilka istotnych trendów, które mogą wpłynąć na zarówno metody ataków, jak i strategie obronne.

Pierwszym trendem jest rosnąca rola sztucznej inteligencji (AI) w cyberatakach. Już dziś dostępne są generatywne modele językowe (jak ChatGPT), które napastnicy mogą wykorzystać do tworzenia bardzo przekonujących i spersonalizowanych wiadomości phishingowych na masową skalę. AI potrafi wygenerować e-mail pozbawiony literówek, idealnie dostosowany stylem do ofiary, co utrudnia odróżnienie go od prawdziwej korespondencji (Jabir i in., 2025). Odnotowano przypadki użycia narzędzi AI do obchodzenia filtrów antyspamowych i antyphishingowych, a nawet do tworzenia fałszywych głosów i nagrań wideo (tzw. deepfake), które mogą posłużyć w atakach typu vishing. Np. przestępcy mogą dzięki syntezie mowy podszyć się przez telefon pod dyrektora firmy i polecić wykonanie przelewu – a głos w słuchawce brzmi niemal nie do odróżnienia od prawdziwego. Takie incydenty już się zdarzają i niewątpliwie ich liczba wzrośnie wraz z doskonaleniem algorytmów generatywnych.

Z drugiej strony, AI staje się także bronią obrońców. Rozwijane są zaawansowane systemy wykrywające phishing z wykorzystaniem uczenia maszynowego, analizujące setki cech wiadomości (lingwistycznych, technicznych) w ułamku sekundy. Sztuczna inteligencja może również pomagać w identyfikacji nietypowych zachowań w sieci (anomaly detection), wspierając analityków bezpieczeństwa w szybszym namierzaniu incydentów. W przyszłości modele AI mogą w czasie rzeczywistym oceniać ryzyko każdego przychodzącego e-maila i ostrzegać użytkownika, np. komunikatem „Uwaga: ta wiadomość jest bardzo podobna do znanego ataku phishingowego". Niemniej, należy pamiętać, że AI to broń obosieczna – będzie wykorzystywana przez obie strony konfliktu, więc prawdopodobnie zobaczymy jednocześnie wzrost wyrafinowania ataków i poprawę narzędzi obronnych.

Kolejnym trendem jest dalsza profesjonalizacja i komercjalizacja cyberprzestępczości. Omówiony wcześniej model Ransomware-as-a-Service jest

częścią szerszego zjawiska Crime-as-a-Service, gdzie usługi do przeprowadzania ataków (nie tylko ransomware, ale też phishing, DDoS, botnety) są sprzedawane jak zwykłe usługi IT (Meland i in., 2020). To oznacza, że próg wejścia dla nowych cyberprzestępców obniża się – mogą kupić potrzebne narzędzia zamiast tworzyć je od zera. Możemy spodziewać się pojawiania kolejnych wyspecjalizowanych „pod-rynunków", np. usług oferujących gotowe kampanie phishingowe na zlecenie, kompletnych pakietów do kradzieży tożsamości itd. Dla obrońców oznacza to konieczność szerszego spojrzenia – zwalczanie poszczególnych grup przestępczych może nie wystarczyć, jeśli na ich miejsce wejdą nowi gracze korzystający z tych samych usług podziemnych.

Ewoluuje również charakter celów ataków. Jeszcze niedawno dominującymi ofiarami ransomware były pojedyncze firmy czy instytucje, atakowane indywidualnie. Teraz coraz częściej przestępcy biorą na celownik łańcuchy dostaw (supply chain) – atakują dostawcę oprogramowania lub usługę chmurową, której awaria implikuje jednoczesny atak na dziesiątki czy setki powiązanych z nią organizacji. Przykładem był wspomniany atak na firmę Kaseya w 2021 r., gdzie poprzez producenta oprogramowania do zarządzania IT zainfekowano setki jego klientów naraz, żądając okupu zbiorczego (Meland i in., 2020). Ten model ataku maksymalizuje zasięg szkód i potencjalny zysk z jednego włamania. Jest wyzwaniem dla obrońców, gdyż wymaga zabezpieczania nie tylko własnej infrastruktury, ale i kontroli bezpieczeństwa u dostawców (co bywa trudne).

Wreszcie, w odpowiedzi na narastającą plagę ataków, władze państwowe i organy ścigania nasilają działania. Coraz częściej słyszymy o międzynarodowych operacjach wymierzonych w grupy ransomware – współpraca policji różnych krajów doprowadziła już do aresztowań członków kilku znanych gangów (np. REvil czy NetWalker). Pojawiają się także inicjatywy prawne: rozważane jest wprowadzenie regulacji zakazujących ofiarom płacenia okupu. Taki zakaz – choć kontrowersyjny – miałby pozbawić przestępców motywacji finansowej (skoro nikt nie zapłaci, ataki stracą sens). Jednak krytycy wskazują, że w praktyce mógłby on karać ofiary i skłaniać firmy do ukrywania ataków zamiast ich zgłaszania. Innym trendem jest rozwój rynku ubezpieczeń cybernetycznych – przedsiębiorstwa wykupują polisy pokrywające

straty związane z atakiem ransomware, włącznie z kwotą okupu. Niestety, pojawiły się obawy, że ubezpieczenia te paradoksalnie napędzają przestępczość (ubezpieczyciel i tak zapłaci okup, więc atakujący chętniej atakują dobrze ubezpieczone podmioty). W odpowiedzi część ubezpieczycieli wprowadza klauzule wyłączające odpowiedzialność za szkody spowodowane np. atakami sponsorowanymi przez państwa (których nie da się przewidzieć ani im zapobiec standardowymi środkami).

Patrząc w przyszłość, należy założyć, że zagrożenia cybernetyczne będą nadal ewoluować i nasilać się. Cyberprzestępcy będą eksplorować nowe wektory ataku (np. urządzenia IoT – wyobraźmy sobie ransomware blokujący inteligentny dom czy samochód), nowe techniki wymuszeń (np. kombinacje ataków fizycznych i cyfrowych), a także będą starali się obchodzić istniejące zabezpieczenia (np. stosując AI do uniknięcia detekcji). Z kolei społeczność zajmująca się bezpieczeństwem będzie rozwijać coraz lepsze narzędzia obrony, standardy i regulacje. Walka będzie toczyć się dalej na zasadzie „kroku naprzód i kroku w tył" po każdej ze stron.

Wnioski

Przegląd najgroźniejszych obecnie cyberataków – phishingu i ransomware (wraz z modelem RaaS) – prowadzi do kilku kluczowych wniosków. Po pierwsze, nawet pozornie mało znaczące incydenty (jak pojedynczy phishingowy e-mail) mogą uruchomić kaskadę zdarzeń skutkujących poważnym kryzysem bezpieczeństwa. Cyberprzestępcy umiejętnie łączą techniki socjotechniczne z malware, aby osiągać swoje cele. Po drugie, skala i profesjonalizacja tych ataków jest obecnie bezprecedensowa – phishing stał się codziennością dla internautów na całym świecie, a ransomware przerodziło się w dochodowy biznes przestępczy o globalnym zasięgu. Po trzecie, konsekwencje ataków wykraczają daleko poza straty cyfrowe: realnie wpływają na życie ludzi, ciągłość działania organizacji i zaufanie do technologii.

Na szczęście zrozumienie metod działania atakujących pozwala na skuteczniejszą obronę. Najważniejsze elementy ochrony to: świadomość i czujność użytkowników (edukacja, szkolenia, kultura bezpieczeństwa), warstwowe zabezpieczenia techniczne (filtry, antywirusy, aktualizacje, backupy, 2FA,

segmentacja) oraz koordynacja działań na poziomie instytucji i państwa (wymiana informacji o zagrożeniach, wspólne ściganie cyberprzestępców, standardy postępowania). Nie ma jednego cudownego rozwiązania – potrzebne jest podejście systemowe, łączące ludzi, procedury i technologie.

Rozwój nowych technologii, takich jak sztuczna inteligencja, przynosi zarówno szanse, jak i zagrożenia w kontekście cyberbezpieczeństwa. Będziemy świadkami coraz bardziej wyrafinowanych ataków (np. phishing wspierany AI, ransomware na IoT) i musimy się na nie przygotować, rozwijając równie zaawansowane metody obrony. Walka z cyberprzestępczością przypomina wyścig – aby go nie przegrać, musimy biec szybciej niż atakujący lub przynajmniej skutecznie reagować na ich ruchy.

Podsumowując, bezpieczeństwo w cyberświecie zależy od wspólnej odpowiedzialności: każdy użytkownik (poprzez ostrożne zachowanie), każda organizacja (poprzez inwestycje w zabezpieczenia i szkolenia) oraz system na poziomie społecznym (prawo, organy ścigania, współpraca międzynarodowa) mają role do odegrania. Tylko synergiczne działania mogą istotnie ograniczyć skalę zagrożeń. Mamy nadzieję, że niniejsze opracowanie przyczyni się do zwiększenia świadomości o naturze ataków phishingowych i ransomware oraz podkreśla znaczenie proaktywnej postawy – tak, aby nie dać się złapać na przynętę w cyfrowym oceanie pełnym zagrożeń.

Literatura

1. Alder, S. (2020). *Hospital ransomware attack results in patient death*. HIPAA Journal.
2. Botchkovar, E., Cui, K., Antonaccio, O., Perkins, R., Maimon, D. (2025). The organized activities of ransomware groups: A social network approach. *Technology in Society*, *82*, 102873. https://doi.org/10.1016/j.techsoc.2025.102873
3. Fisher, T., Pieri, Z., Howell, C. J., O'Malley, R., Tremblay, L., Dawoud, M. (2025). Vendor communication themes in darknet Ransomware-as-a-Service (RaaS) advertisements. *Computers in Human Behavior*, *165*, 108571. https://doi.org/10.1016/j.chb.2025.108571
4. Jabir, R., Le, J., Nguyen, C. (2025). Phishing attacks in the age of generative artificial intelligence: A systematic review of human factors. *AI, 6*(8), 174. https://doi.org/10.3390/ai6080174

5. López-Aguilar, P., Urruela, C., Batista, E., Machin, J., Solanas, A. (2025). Phishing vulnerability and personality traits: Insights from a systematic review. *Computers in Human Behavior Reports, 20*, 100784. https://doi.org/10.1016/j.chbr.2025.100784
6. Malik, A., Khan, B., Qaisar, S. M., Krichen, M. (2025). AntiPhishX: An AI-driven service-oriented ensemble framework for detecting phishing and ai-powered phishing attacks. *Information and Software Technology, 188*, 107877. https://doi.org/10.1016/j.infsof.2025.107877
7. Meland, P. H., Bayoumy, Y. F. F., Sindre, G. (2020). The ransomware-as-a-service economy within the darknet. *Computers Security, 92*, 101762. https://doi.org/10.1016/j.cose.2020.101762
8. Zhang, C., Luo, F. (2025). Bargaining game theoretical analysis framework for ransomware attacks. *Journal of Information Security and Applications, 93,* 104115. https://doi.org/10.1016/j.jisa.2025.104115

Netografia

1. CECOM CIO G6 Cybersecurity (2024). *Secure our world – CECOM raises awareness about phishing*. Army.mil. Pobrane z: https://www.army.mil/article/280696/secure_our_world_cecom_raises_awareness_about_phishing (data dostępu: 10.09.2025).
2. GOV.UK. (2025). Cyber Security Breaches Survey 2025: Technical report. Gov.uk. Pobrane z: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025-technical-report (data dostępu: 10.09.2025).