Praca doktorska

Wpływ incydentów cyberbezpieczeństwa na krótkoterminową wycenę przedsiębiorstw

mgr Konrad Sałek

Abstrakt

Celem niniejszej pracy doktorskiej jest zbadanie krótkoterminowego wpływu incydentów cyberbezpieczeństwa na wartość rynkową przedsiębiorstw notowanych na giełdzie. W dobie dynamicznej cyfryzacji gospodarki i narastającej liczby ataków cybernetycznych problematyka ich ekonomicznych skutków nabiera kluczowego znaczenia dla stabilności rynków finansowych. Cyberataki, takie jak ransomware, wycieki danych czy ataki typu DDoS, powodują nie tylko bezpośrednie straty finansowe, lecz także utratę reputacji i zaufania inwestorów, co przekłada się na wycenę rynkową spółek.

W pracy wykorzystano metodę event study, powszechnie stosowaną w analizach reakcji rynków kapitałowych na wystąpienie określonych zdarzeń. Procedura badawcza obejmowała wyznaczenie okna bazowego, służącego do oszacowania parametrów modelu rynkowego, oraz okna zdarzenia, obejmującego okres przed i po ujawnieniu incydentu cyberataków. Na tej podstawie obliczono nadzwyczajne stopy zwrotu (AR) oraz skumulowane nadzwyczajne stopy zwrotu (CAR) dla analizowanych spółek. Dla oceny istotności reakcji rynkowej zastosowano test t-Studenta, umożliwiający weryfikację hipotezy badawczej dotyczącej negatywnego wpływu ujawnienia incydentu na wartość rynkową przedsiębiorstwa. Przeprowadzona analiza empiryczna potwierdziła, że informacje o wystąpieniu incydentów cyberbezpieczeństwa prowadzą do statystycznie istotnych, ujemnych skumulowanych nadzwyczajnych zwrotów w krótkim okresie po zdarzeniu. Wyniki te dowodzą, iż rynki kapitałowe szybko i negatywnie reagują na doniesienia o cyberatakach, traktując je jako czynnik ryzyka wpływający na ocenę kondycji finansowej i wiarygodności spółek.

Wkład pracy ma charakter zarówno teoretyczny, jak i praktyczny. Po stronie teoretycznej rozszerza ona krajowy dorobek naukowy w zakresie finansów i zarządzania ryzykiem o analizę ilościową wpływu cyberataków na wartość rynkową przedsiębiorstw. W wymiarze praktycznym wnioski mogą stanowić podstawę dla opracowania skuteczniejszych strategii zarządzania ryzykiem cybernetycznym oraz procedur reagowania na incydenty w przedsiębiorstwach i instytucjach finansowych.

Słowa kluczowe: cyberbezpieczeństwo, cyberatak, wyciek danych, event study, nadzwyczajne stopy zwrotu (AR), skumulowane nadzwyczajne stopy zwrotu (CAR), test t-Studenta, ryzyko rynkowe.

Abstract

The objective of this doctoral dissertation is to examine the short-term impact of cybersecurity incidents on the market valuation of publicly listed companies. In an era of increasing digitalisation and growing dependence on information systems, the economic consequences of cyberattacks have become a key issue for the stability of financial markets. Attacks such as ransomware, data breaches and distributed denial-of-service (DDoS) incidents generate not only direct financial losses but also reputational damage and a decline in investor confidence, which in turn affects firms' market value.

The research applies the event study methodology, which enables the quantitative assessment of market reactions to specific events. The procedure includes defining an estimation window to determine the parameters of the market model and an event window covering the period before and after the disclosure of a cybersecurity incident. Based on these data, abnormal returns (AR) and cumulative abnormal returns (CAR) were calculated for the affected companies. The Student's t-test was employed to verify the statistical significance of the differences between actual and expected returns, allowing for the testing of the hypothesis that the disclosure of a cyberattack has a negative impact on short-term market value. The empirical results confirm that announcements of cybersecurity incidents lead to statistically significant negative cumulative abnormal returns in the short term following the event. These findings demonstrate that capital markets react rapidly and adversely to information about cyberattacks, perceiving them as a risk factor affecting firms' financial performance and credibility.

The dissertation contributes to both theory and practice. Theoretically, it enriches Polish-language empirical research in finance and risk management by providing a quantitative short-term assessment of the economic effects of cybersecurity incidents. Practically, the findings may support the development of more effective cyber-risk management strategies and incident-response frameworks aimed at protecting corporate market value.

Keywords: cybersecurity, cyberattack, data breach, event study, abnormal returns (AR), cumulative abnormal returns (CAR), Student's t-test, market risk.

Spis treści

WSTĘP

Wraz z postępem technologii cyfrowych i rosnącą zależnością gospodarki od systemów informatycznych, cyberbezpieczeństwo stało się jednym z kluczowych zagadnień w nowoczesnym zarządzaniu ryzykami podmiotów gospodarczych[1]. Cyberataki, które można zdefiniować jako celowe działania ukierunkowane na uszkodzenie systemów komputerowych, zakłócenie procesów cyfrowych bądź kradzież danych, zazwyczaj niosą za sobą poważne skutki dla codziennego funkcjonowania firm, instytucji publicznych oraz konsumentów[2]. W dobie globalizacji i rewolucji cyfrowej bezpieczeństwo cybernetyczne staje się nie tylko priorytetem dla firm z sektora finansowego i technologicznego. Również instytucje rządowe oraz organizacje medyczne czy edukacyjne zaczynają doceniać jej znaczenie[3]. Wielkość i poufność przetwarzanych danych oraz coraz liczniejsze ataki cybernetyczne sprawiają, że każdy incydent czy wyciek informacji odzwierciedla się postaci poważnych strat finansowych i szkód dla reputacji[4].

Jak wskazują raporty branżowe koszty, które są wynikiem cyberataków rosną z każdym rokiem. Podmioty coraz częściej podejmują decyzje o inwestowaniu w różne systemy ochrony[5]. Jednak należy zwrócić uwagę, że stale zmieniające się techniki ataków powodują, że skuteczność tych działań jest ograniczona. Współczesne incydenty związane z cyberbezpieczeństwem, do których można zaliczyć *ransomware*, wycieki danych czy ataki typu DDoS (*Distributed Denial of Service*), są jednymi z najczęściej zgłaszanych zagrożeń. Wraz z rozwojem technologii informatycznych rośnie również liczba potencjalnych wektorów ataków[6]

---

[1] Carrillo, E. F. P. (2023). *Cybersecurity in European Financial Institutions: New Grounds for Corporate Governance Reform*. *European Business Law Review*.

[2] Erkan-Barlow, A., Ngo, T., Goel, R., & Streeter, D. (2023). An in-depth analysis of the impact of cyberattacks on the profitability of commercial banks in the United States. *Journal of Global Business Insights*. https://doi.org/10.5038/2640-6489.8.2.1246.

[3] Wolff, J., & Lehr, W. (2018). When Cyber Threats Loom, What Can State and Local Governments Do?. *Georgetown Journal of International Affairs*, 19, 67 - 75. https://doi.org/10.1353/GIA.2018.0008.

[4] K. Kopp, C. Kaffenberger, M. Wilson, „Cyber Risk Measurement and the Holistic Impact of Cyberattacks", „Journal of Cybersecurity", 2017, nr 3 (1), s. 13.

[5] J. C. Smith, „The True Cost of Cyber Attacks: Trends and Impacts", „Cybersecurity Review", 2023, nr 3 (15), s. 45-47.

[6] **Wektor ataku** to ścieżka lub metoda, którą cyberprzestępcy wykorzystują do uzyskania nieautoryzowanego dostępu do systemów, sieci lub danych.

– w szczególności w obszarach takich jak handel algorytmiczny, technologie mobilne, chmury obliczeniowe i Internetu Rzeczy (IoT). Ponadto, ostatnie lata obfitują w wykorzystywanie cyberataków jako narzędzia walki gospodarczej i geopolitycznej, gdzie celem ataków są nie tylko prywatne firmy, lecz także instytucje państwowe i infrastruktura krytyczna[7].

W literaturze z obszaru finansów[8] od dawna przedmiotem badań są kwestie, w jaki sposób rynki reagują na różne incydenty i kryzysy, takie jak katastrofy naturalne, skandale korupcyjne czy kryzysy finansowe. Incydenty o charakterze cyberataków, które należy identyfikować jako jedną z najnowszych form zakłóceń gospodarczych, mogą wywoływać istotne reakcje ze strony rynków z uwagi na fakt, iż w wielu przypadkach prowadzą do bezpośrednich strat finansowych, utraty danych, czy spadku zaufania ze strony inwestorów i klientów. Istniejące badania, oparte na analizie *event study*, jasno wskazują, że rynki finansowe szybko reagują na informacje o różnych rodzajach incydentów. Analiza *event study* pozwala na ocenę krótkoterminowych reakcji rynkowych poprzez porównanie rzeczywistych zwrotów z oczekiwanymi, co umożliwia wyłonienie tzw. efektów „nadzyczajnych", wynikających z ujawnienia incydentu cyberataku lub innego zdarzenia, które może być uznane jako kryzysowe[9].

Zrozumienie wpływu cyberataków na wartość rynkową firm odgrywa kluczową rolę w podejmowaniu decyzji związanych z zarządzaniem ryzykiem oraz inwestycjami w cyberbezpieczeństwo. Coraz większa złożoność ataków i ich potencjalne konsekwencje powodują, że niektóre przedsiębiorstwa – w zależności od specyfiki działalności, charakterystyki klientów czy stopnia uzależnienia od przetwarzania danych – są bardziej narażone na straty niż inne. Badanie tych zagadnień pozwoli lepiej zrozumieć potencjalne skutki takich incydentów, aby opracować skuteczne strategie reagowania na cyberzagrożenia.

W niniejszej pracy autor dokonuje analizy dotyczącej krótkoterminowego wpływu cyberataków na wartość rynkową firm notowanych na giełdzie przy użyciu metody *event study*.

[7] S. J. Brown, J. B. Warner, „Using Daily Stock Returns: The Case of Event Studies", „Journal of Financial Economics", 1985, nr 14 (3), s. 7

[8] Sasikumar, S., & Sundaram, N. (2024). Event study methodology trends in the stock market: A systematic review based on bibliometric analysis. *Multidisciplinary Reviews*. https://doi.org/10.31893/multirev.2024234.

[9] A. C. MacKinlay, „Event Studies in Economics and Finance", „Journal of Economic Literature", 1997, nr 35 (1), s. 13

Celem badania jest weryfikacja, czy ujawnienie cyberataku powoduje istotnie negatywną reakcję rynku, co znajduje odzwierciedlenie w ujemnych skumulowanych nadzwyczajnych zwrotach (CAR - *Cumulative Abnormal Returns*) w okresie po incydencie. W analizie z wykorzystaniem metody *event study* wpływ incydentów cyberbezpieczeństwa na krótkoterminową wycenę przedsiębiorstw wyraża się poprzez nadzwyczajne stopy zwrotu (*Abnormal Returns*, AR) oraz skumulowane nadzwyczajne stopy zwrotu (CAR).

Autor postawił następującą hipotezę badawczą : „*Cyberataki mają istotnie negatywny wpływ na krótkoterminową wartość rynkową firm notowanych na giełdzie, co znajduje odzwierciedlenie w ujemnych wartościach skumulowanych nadzwyczajnych zwrotów (CAR) po ujawnieniu incydentu”*.

Wybór krótkoterminowego zakresu czasowego w analizie wpływu cyberataków wynika z faktu, iż zmiany wartości rynkowej w krótkim okresie są bardziej mierzalne w danych giełdowych, ponieważ ich przebieg nie jest jeszcze zakłócony przez inne zmienne makroekonomiczne. Krótkoterminowe badania pozwalają więc zmierzyć bezpośredni wpływ incydentów takich jak ataki cybernetyczne na zachowania rynków finansowych[10]. W ramach przeprowadzonej analizy uwzględniono dwa kluczowe okresy: okno bazowe, w którym szacowane są parametry modelu rynkowego oraz okno zdarzenia, obejmujące czas przed i po ujawnieniu cyberataku. Okno bazowe pozwala na dokładne określenie oczekiwanych zwrotów, podczas gdy okno zdarzenia umożliwia obserwację bezpośrednich reakcji rynkowych[11]. Do analizy autor wykorzystał metodę *event study* która jest powszechnie wykorzystywana do analizy krótkoterminowych reakcji na konkretne wydarzenia. Dzięki zastosowanej metodzie możliwe jest porównanie rzeczywistych zwrotów z akcji przedsiębiorstw z oczekiwanymi zwrotami w warunkach braku danego zdarzenia. Umożliwia to wskazanie tzw. nadzwyczajnych zwrotów (AR) oraz ich skumulowanej wartości (CAR), co stanowi podstawę oceny wpływu incydentów na rynki finansowe[12].

[10] E. F. Fama, „Market Efficiency, Long-Term Returns, and Behavioral Finance”, „Journal of Financial Economics”, 1998, nr 49 (2), s. 283.
[11] J. Y. Campbell, A. W. Lo, A. C. MacKinlay, „The Econometrics of Financial Markets”, Princeton University Press, 1997, s. 131.
[12] S. J. Brown, J. B. Warner, „Using Daily Stock Returns: The Case of Event Studies”, „Journal of Financial Economics”, 1985, nr 14 (3), s. 7.

Analiza przy użyciu metody Event Study została uzupełniona o zastosowanie testu t-Studenta jako narzędzia statystycznego. Za jego pomocą możliwa jest ocena istotności różnic między nadzwyczajnymi stopami zwrotu (AR) a stopami oczekiwanymi, co pozwala zweryfikować hipotezę o negatywnym wpływie cyberataków na wartość rynkową przedsiębiorstw. W niniejszym badaniu test t zostanie zastosowany do skumulowanych nadzwyczajnych stóp zwrotu (CAR), w celu sprawdzenia, czy ujawnienie cyberataku wywołuje istotnie ujemną reakcję rynku w krótkim okresie po incydencie[13].

teoretycznego kontekstu dla badania wpływu cyberataków na wartość rynkową przedsiębiorstw. Dotychczasowe prace wskazują, że incydenty takie jak wycieki danych czy ransomware mogą prowadzić do natychmiastowych spadków wartości rynkowej firm notowanych na giełdzie — zarówno na skutek utraty zaufania inwestorów, jak i potencjalnych strat finansowych[14]. W literaturze podkreśla się, że skala reakcji rynkowej zależy od takich czynników jak wielkość incydentu, reakcja firmy czy percepcja ryzyka przez rynek — jednak brak konsensusu co do jej jednolitego charakteru wskazuje na potrzebę dalszych[15]. Przegląd literatury pozwolił autorowi na identyfikację dominujących podejść badawczych — między innymi zastosowania metody event study do pomiaru krótkoterminowych reakcji rynkowych — oraz wskazuje na konieczność uogólnienia wniosków dotyczących wpływu cyberataków na rynki finansowe. Zastosowane w pracy metody umożliwiają wszechstronne zrozumienie wpływu cyberataków na rynki kapitałowe i mogą stanowić podstawę do opracowania praktycznych rekomendacji dla przedsiębiorstw, inwestorów oraz organów nadzorczych w świetle rosnących zagrożeń związanych z cyberbezpieczeństwem.

Współczesna gospodarka cyfrowa charakteryzuje się coraz większą zależnością przedsiębiorstw od systemów informatycznych, co sprawia, że problematyka cyberbezpieczeństwa nabiera strategicznego znaczenia dla stabilności rynków finansowych i funkcjonowania całych gospodarek. Wraz ze wzrostem skali cyfryzacji i rosnącą

---

[13] Kothari S.P., Warner J.B., *Econometrics of Event Studies*, [w:] *Handbook of Corporate Finance: Empirical Corporate Finance*, B. E. Eckbo (red.), Elsevier, Amsterdam 2006, s. 3-36. DOI:10.1016/B978-0-444-53187-6.50002-8.

[14] Arcuri M. C., Brogi M., Gandolfi G., *The effect of cyber-attacks on stock returns*, Corporate Ownership & Control, vol. 15(2), 2018, s. 70-83. DOI:10.22495/cocv15i2art6.

[15] Tosun O. K., *Cyber Attacks and Stock Market Activity*, International Review of Financial Analysis, vol. 76, 2021, art. 101795. DOI:10.1016/j.irfa.2021.101795

częstotliwością incydentów cybernetycznych rośnie również potrzeba prowadzenia badań empirycznych, które pozwalają uchwycić ekonomiczne skutki tych zjawisk w sposób ilościowy i mierzalny.

Dotychczasowa literatura międzynarodowa, mimo rosnącego zainteresowania tematyką cyberbezpieczeństwa, koncentruje się głównie na długoterminowych skutkach cyberataków — takich jak wpływ na wyniki finansowe, reputację, ryzyko operacyjne czy koszt kapitału. Badania oparte na danych krótkookresowych, w których analizowane są bezpośrednie reakcje rynków kapitałowych na ujawnienie informacji o incydencie, pozostają wciąż stosunkowo nieliczne. Nieliczne prace empiryczne oparte na metodzie event study[16][17][18] wykazują, że w krótkim horyzoncie czasowym rynki reagują negatywnie na informacje o cyberatakach, co przejawia się w spadkach stóp zwrotu spółek dotkniętych incydentem. Wyniki te wskazują, że cyberataki stanowią istotny czynnik ryzyka rynkowego, a reakcje inwestorów mają często natychmiastowy charakter. Pomimo rosnącej liczby badań na poziomie globalnym, w literaturze polskojęzycznej wciąż brakuje opracowań empirycznych poświęconych wpływowi incydentów cyberbezpieczeństwa na wartość rynkową przedsiębiorstw. Analizy oparte na metodzie event study nie były dotąd szerzej wykorzystywane w badaniach nad konsekwencjami cyberataków na polskim rynku kapitałowym. Luka ta wskazuje na potrzebę wprowadzenia ilościowych badań nad wpływem cyberzagrożeń na rynki finansowe do polskiego dyskursu naukowego, co stanowi jeden z kluczowych celów niniejszej pracy. Prezentowana dysertacja podejmuje próbę wypełnienia tej luki poprzez analizę krótkoterminowego wpływu cyberataków na wartość rynkową spółek notowanych na giełdzie z wykorzystaniem metody event study. Zastosowana metodologia pozwala na precyzyjne uchwycenie reakcji rynków finansowych w okresie bezpośrednio po ujawnieniu informacji o incydencie, przy jednoczesnym ograniczeniu wpływu czynników zewnętrznych, które w dłuższym okresie

---

[16] **Corbet, S., Larkin, C., Lucey, B.** *HACKED: Understanding the Stock Market Response to Cyberattacks*, *Finance Research Letters*, 2023. DOI: 10.1016/j.frl.2023.104206.

[17] **Tosun, O. K.** *Cyber Attacks and Stock Market Activity*, *International Review of Financial Analysis*, 76, 2021, art. 101795. DOI: 10.1016/j.irfa.2021.101795.

[18] **Arcuri, M. C., Brogi, M., Gandolfi, G.** *The Effect of Cyber-Attacks on Stock Returns*, *Corporate Ownership & Control*, 15(2), 2018, s. 70–83. DOI: 10.22495/cocv15i2art6

mogłyby zniekształcać wyniki analizy. Zastosowanie miary nadzwyczajnych stóp zwrotu (Abnormal Returns, AR) oraz ich skumulowanych wartości (Cumulative Abnormal Returns, CAR) umożliwia ilościowe określenie siły i kierunku reakcji rynkowej. Ponadto wykorzystanie testu t-Studenta pozwala na statystyczną weryfikację hipotezy o istotnym negatywnym wpływie cyberataków na krótkoterminową wartość rynkową przedsiębiorstw. Wyniki przeprowadzonej analizy mogą stanowić istotny wkład w rozwój krajowych badań empirycznych z zakresu finansów i zarządzania ryzykiem, a także przyczynić się do pogłębienia rozumienia ekonomicznych konsekwencji cyberzagrożeń. Z perspektywy praktycznej, uzyskane rezultaty mogą zostać wykorzystane do opracowania skuteczniejszych strategii zarządzania ryzykiem cybernetycznym oraz ochrony wartości rynkowej firm, szczególnie w warunkach coraz większej ekspozycji na incydenty w przestrzeni cyfrowej.

Struktura pracy obejmuje cztery rozdziały. W rozdziale pierwszym autor omawia zagadnienia związane z cyberbezpieczeństwem i cyberatakami, w tym ich gospodarcze skutki i wpływ na przedsiębiorstwa. W drugim rozdziale skupiono się na rynku finansowym oraz jego podatności na cyberataki, ze szczególnym uwzględnieniem różnych segmentów i ryzyka związanego z handlem algorytmicznym. W trzeci rozdziale opisano metodykę badań oraz wyniki przeprowadzonej analizy *event study*, uwzględniając zebranie danych, ustalanie okna bazowego i zdarzenia, a także obliczanie nadzwyczajnych zwrotów. Bazując na uzyskanych w rozdziale 3 wynikach badań, rozdział czwarty zawiera opis sposoby zapewnienia cyberbezpieczeństwa, takich jak regulacje prawne oraz standardy międzynarodowe. Pracę kończy podsumowanie wyników oraz rekomendacje dotyczące zarządzania ryzykiem cybernetycznym w kontekście ochrony wartości rynkowej firm.

W niniejszej pracy autor podejmuje próbę dokonania analizy krótkoterminowego wpływu cyberataków na wartość rynkową firm z różnych sektorów, wykorzystując głównie metodę *event study*. W kontekście wzrostu liczby i złożoności cyberataków szczególnie istotne jest zrozumienie, w jaki sposób inwestorzy reagują na incydenty cybernetyczne. Rezultaty przeprowadzonej analizy mogą okazać się cenne dla przedsiębiorstw, inwestorów oraz decydentów, którzy poszukują skutecznych strategii zarządzania ryzykiem i ochrony wartości rynkowej swoich firm.

ROZDZIAŁ I. CYBERBEZPIECZEŃSTWO I CYBERATAKI – SKUTKI GOSPODARCZE

1. Def nicja cyberataku i cyberbezpieczeństwa

Cyberbezpieczeństwo i cyberataki stają się jednymi z kluczowych zagadnień we współczesnej gospodarce cyfrowej. Cyberbezpieczeństwo można zdefiniować jako zestaw praktyk, technologii i procesów mających na celu ochronę systemów komputerowych, sieci, oprogramowania oraz danych przed nieuprawnionym dostępem, uszkodzeniem lub zniszczeniem. Należy je rozpatrywać jako zagadnienie wielodziedzinowe obejmujące zarówno aspekty techniczne, jak i organizacyjne, prawne oraz edukacyjne. Definicja ta jest zgodna z interpretacjami międzynarodowych standardów, takich jak chociażby wytyczne NIST (*National Institute of Standards and Technology*), które definiują cyberbezpieczeństwo jako *„ochronę systemów informacyjnych przed zagrożeniami cybernetycznymi oraz zapobieganie ich wpływowi na poufność, integralność i dostępność danych”*[19].

Cyberatak definiowany jest jako celowe działanie wymierzone w systemy komputerowe, sieci lub dane, mającym na celu ich uszkodzenie, przejęcie kontroli nad nimi lub kradzież informacji[20]. Cyberataki posiadają rozbudowaną typologię- można tu zaliczyć m.in.: ataki typu *ransomware*, wycieki danych osobowych, ataki typu DDoS czy phishing. Należy przy tym zaznaczyć, że istotnym elementem cyberataku jest intencjonalność działań sprawcy, które mają na celu wywołanie określonych skutków – zarówno w sferze ekonomicznej jak i społecznej[21].

Cyberbezpieczeństwo stało się priorytetowym obszarem dla przedsiębiorstw, instytucji publicznych oraz osób prywatnych. W szczególności przedsiębiorstwa z sektora finansowego i technologicznego stają pod rosnącą presją ze strony coraz bardziej zaawansowanych zagrożeń,

[19] P. W. Singer, A. Friedman, „Cybersecurity and Cyberwar: What Everyone Needs to Know”, Oxford University Press, 2014, s. 11.

[20] Kadivar M., *Cyber-Attack Attributes: Examining Definitions of Cyber-Attacks from the Literature and High-Profile Incidents*, *Technology Innovation Management Review*, vol. 4(11), 2014.

[21] E. M. Hutchins, M. J. Cloppert, R. M. Amin, „Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains”, „Lockheed Martin Corporation”, 2011, s. 5.

które mogą powodować utratę danych, przerwy w działalności operacyjnej oraz duże straty finansowe. W literaturze zwraca się uwagę, że cyberataki stają się coraz bardziej złożone i trudne do wykrycia, co sprawia, że wymagania wobec systemów cyberbezpieczeństwa stale rosną[22].

Omawiając definicję warto również zwrócić uwagę na mnogość podejść do cyberbezpieczeństwa w zależności sektora gospodarki. Na przykład w sektorze finansowym działania zapewniające cyberbezpieczeństwo skupiają się przede wszystkim na ochronie danych transakcyjnych i przeciwdziałaniu oszustwom. Z kolei w sektorze infrastruktury krytycznej kluczowe jest zapobieganie zakłóceniom działania systemów kontrolnych i operacyjnych. Tak szerokie podejście do ochrony środowiska cyfrowego powoduje, że cyberbezpieczeństwo jest dziedziną interdyscyplinarną, wymagającą współpracy ekspertów z różnych obszarów, takich jak informatyka, prawo, ekonomia czy edukacja[23].

Cyberatak i cyberbezpieczeństwo to dwie komplementarne strony tego samego procesu – z jednej strony narzędzie destrukcji, a z drugiej konieczność budowania systemów ochrony, które stają się niezbędnym elementem w codziennym funkcjonowaniu współczesnych organizacji w gospodarce informacyjnej. Warto zauważyć, że definicje cyberbezpieczeństwa i cyberataków podlegają procesowi ewolucji wraz z rozwojem czynnika technologicznego oraz wzrostem liczby i różnorodności zagrożeń. W literaturze przedmiotu coraz częściej podkreśla się, że cyberbezpieczeństwo to nie tylko ochrona infrastruktury technicznej, lecz także zarządzanie ryzykiem związanym z działalnością w środowisku cyfrowym. Według jednej z szeroko uznawanych definicji, cyberbezpieczeństwo obejmuje „zarządzanie bezpieczeństwem informacji w kontekście technologii cyfrowych, a także mechanizmy organizacyjne i edukacyjne wspierające te działania”[24].

Podobnie pojęcie cyberataków nie ogranicza się jedynie do działań o charakterze technicznym. Współczesne cyberataki coraz częściej łączą technologie cyfrowe z elementami psychologicznymi, jak w przypadku phishingu lub manipulacji danymi, które mają na celu wywołanie określonych zachowań użytkowników. Przykładowo, ataki typu *ransomware* nie

[22] C. Kopp, C. Kaffenberger, M. Wilson, „Cyber Risk Measurement and the Holistic Impact of Cyberattacks”, „Journal of Cybersecurity”, 2017, nr 3 (1), s. 13
[23] K. E. Himma, „The Ethics of Cybersecurity”, Springer, 2021, s. 27
[24] P. Cornish, „The Cybersecurity Lexicon”, Routledge, 2017, s. 34

tylko zakłócają działanie systemów komputerowych, ale również wymuszają na ofiarach określone działania, takie jak zapłata okupu w kryptowalutach[25].

Ewolucja cyberzagrożeń wywołuje zmiany w podejściu do cyberbezpieczeństwa jako elementu strategii gospodarczej. Organizacje coraz częściej traktują inwestycje w bezpieczeństwo cyfrowe jako integralną część zarządzania ryzykiem. W szczególności przedsiębiorstwa z branży finansowej, technologicznej i energetycznej muszą uwzględniać cyberbezpieczeństwo w swoich planach operacyjnych, ponieważ brak skutecznej ochrony może prowadzić do poważnych konsekwencji ekonomicznych i reputacyjnych. Raporty branżowe wskazują, że koszty związane z cyberatakami rosną z każdym rokiem, co zmusza organizacje do zwiększania nakładów na systemy ochrony, edukację pracowników oraz współpracę z zewnętrznymi ekspertami ds. cyberbezpieczeństwa[26]. Jednocześnie ważnym aspektem definiowania cyberataków i cyberbezpieczeństwa jest ich międzynarodowy wymiar. Cyberprzestępczość nie zna granic, co sprawia, że współpraca międzynarodowa oraz harmonizacja przepisów prawnych stają się kluczowymi elementami skutecznej walki z zagrożeniami. Organizacje o charakterze międzynarodowym takie jak NATO czy ONZ podkreślają, że cyberbezpieczeństwo powinno być postrzegane jako wspólne dobro międzynarodowe, które wymaga zintegrowanych działań na poziomie globalnym[27].

Podsumowując, zarówno cyberatak, jak i cyberbezpieczeństwo to pojęcia o dynamicznie zmieniającym się znaczeniu, które odzwierciedlają zmieniające się wyzwania współczesnego świata cyfrowego. Ich zrozumienie jest niezbędne nie tylko dla skutecznego zarządzania ryzykiem w organizacjach, ale również dla tworzenia polityk bezpieczeństwa na poziomie państw i społeczności międzynarodowej. W kolejnych częściach pracy autor omawia szczegółowo gospodarcze skutki cyberataków, które stanowią jedne z najistotniejszych konsekwencji współczesnych zagrożeń w świecie cyfrowym.

2. Rodzaje cyberataków

Cyberataki obejmują różnorodne działania wymierzone w systemy informatyczne, sieci oraz dane, mające na celu ich uszkodzenie, przejęcie kontroli lub kradzież informacji. Według

[25] T. Rid, „Cyber War Will Not Take Place", Oxford University Press, 2013, s. 45.
[26] A. Von Solms, R. Von Solms, „Information Security Governance", Springer, 2018, s. 62.
[27] K. Geers, „Strategic Cyber Security", NATO Cooperative Cyber Defence Centre of Excellence, 2011, s. 19.

Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA) najbardziej rozpowszechnione rodzaje cyberataków to *phishing*, ransomware, ataki DDoS, wycieki danych, a także coraz częściej obserwowane ataki na łańcuchy dostaw oraz te wykorzystujące sztuczną inteligencję[28].

Phishing

Phishing to jedna z najpowszechniej stosowanych form ataków cybernetycznych, polegająca na podszyciu się przez sprawcę pod zaufaną osobę, instytucję lub usługę w celu wyłudzenia poufnych informacji (takich jak dane logowania, numery kart płatniczych, dane osobowe) lub skłonienia ofiary do wykonania określonej akcji (na przykład kliknięcia w link, pobrania załącznika czy przekazania informacji) prowadzącej do naruszenia bezpieczeństwa[29]. Mechanizm działania phishingu najczęściej obejmuje wiadomość e-mail, SMS bądź komunikat w aplikacji, który wygląda na autentyczny i pochodzi od podmiotu znanego użytkownikowi, a jego celem jest osłabienie czujności lub pokierowanie użytkownika na fałszywą stronę internetową lub pod złośliwy link. Charakterystycznym elementem ataku jest zastosowanie technik socjotechnicznych — sprawca wykorzystuje zaufanie, pośpiech, emocje lub autorytet, by skłonić użytkownika do działania niezgodnego z jego najlepszym interesem. W literaturze podkreśla się, że phishing stanowi nadal jedno z największych zagrożeń cybernetycznych dla organizacji i użytkowników końcowych — niezależnie od wielkości organizacji, ponieważ jest skuteczny, stosunkowo tani w realizacji i rozwija się wraz z nowymi kanałami komunikacji (SMS, komunikatory, media społecznościowe). Ponadto phishing może przybierać różne formy i wektory ataku – od masowych wiadomości typu „spray-and-pray", przez ataki ukierunkowane (spear-phishing) na konkretne osoby lub organizacje, po nowsze formy jak smishing (phishing przez SMS) czy vishing (phishing przez telefon) – co świadczy o jego rosnącej złożoności i adaptacyjności sprawców[30]. W kontekście organizacyjnym, skutki phishingu obejmują nie tylko wyciek danych czy straty finansowe, lecz także naruszenie reputacji, koszty związane z reakcją na incydent oraz potencjalne zakłócenia działalności

[28] ENISA, *Threat Landscape 2022: Cyber Threats and Trends*, Publications Office of the European Union, 2022, s. 14-16.

[29] Alkhalil Z., Hewage C., Nawaf L., Khan I., *Phishing Attacks: A Recent Comprehensive Study and a New Anatomy*, *Frontiers in Computer Science*, vol. 3, 2021, art. 563060. DOI: 10.3389/fcomp.2021.563060.

[30] Lallie H. et al., *How Good Are We at Detecting a Phishing Attack? Investigating the phishing email threat landscape*, *Plos One* (open access), 2022.

operacyjnej – co czyni tę formę ataku kluczowym elementem zarządzania ryzykiem cybernetycznym w przedsiębiorstwach.

Ransomware

Ransomware jest szczególną formą złośliwego oprogramowania (malware), która po zainfekowaniu systemu ofiary szyfruje dane lub blokuje dostęp do zasobów informatycznych, po czym wymaga zapłaty okupu w zamian za przywrócenie dostępu lub odszyfrowanie tych danych. Przestępca może również grozić publikacją lub sprzedażą wykradzionych informacji, jeżeli okup nie zostanie zapłacony. Incydenty ransomware w ostatnich latach stały się jednym z najpoważniejszych zagrożeń w cyberprzestrzeni — zwłaszcza w odniesieniu do operatorów infrastruktury krytycznej, takich jak systemy energetyczne, transportowe czy łańcuchy dostaw. Przykładem jest atak na Colonial Pipeline w 2021 r., który spowodował poważne zakłócenia w dostawach paliwa w USA i wymusił zapłatę okupu przez operatora systemu. kontekście analizy ekonomicznej i rynkowej istotne jest, że ransomware wywołuje nie tylko straty bezpośrednie (koszty przywrócenia działania, zapłaty okupu), lecz może także prowadzić do: utraty reputacji, zakłóceń operacyjnych, przerw w działalności gospodarczej, wzrostu ryzyka regulacyjnego czy wzmożonej uważności inwestorów i rynków kapitałowych — co czyni ją zagadnieniem istotnym także z perspektywy wpływu na wartość rynkową przedsiębiorstw.[31].

Ataki DDoS (Distributed Denial of Service)

Atak typu Distributed Denial of Service (DDoS) polega na celowym zalewaniu systemu komputerowego, sieci lub usługi bardzo dużą liczbą sztucznych żądań, wysyłanych z wielu źródeł jednocześnie, co powoduje przeciążenie zasobów docelowych (np. przepustowości łącza, mocy obliczeniowej, połączeń sieciowych) i w rezultacie uniemożliwia dostęp prawowitym użytkownikom lub funkcjonowanie usługi. Charakterystyczne jest to, że ruch atakujący pochodzi nie z jednej maszyny, lecz z wielu – często z tysięcy lub nawet milionów źródeł (botnetów, zainfekowanych urządzeń IoT, reflektorów/amplifikatorów) – co znacznie utrudnia jego identyfikację i obronę.Ataki DDoS bywają wykorzystywane jako narzędzie

[31] Cybersecurity and Infrastructure Security Agency (CISA), „The Attack on Colonial Pipeline: What We've Learned, What We've Done Over the Past Two Years”, 2023, dostęp:2025.03.14 https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

destabilizacji operacyjnej — zarówno w cyberprzestępczości (np. wymuszenia okupu, „ransom-DDoS"), jak i w kontekście działań politycznych, ekonomicznych lub geopolitycznych. Ich skuteczność wynika m.in. z możliwości skoordynowanego działania wielu źródeł ruchu oraz wykorzystania technik wzmacniania/refleksji (amplification/ reflection) – co pozwala generować bardzo duży ruch przy relatywnie niewielkich zasobach atakującego[32]. Przykładem ekstremalnego incydentu jest atak na platformę GitHub w dniu 28 lutego 2018 roku, który osiągnął szczytowy poziom około 1,35 terabita na sekundę (Tbps) ruchu — co czyni go jednym z największych udokumentowanych ataków DDoS w historii internetu[33]. W kontekście zarządzania ryzykiem cybernetycznym dla przedsiębiorstw i instytucji, ataki DDoS stanowią poważne zagrożenie: mogą prowadzić do utraty przychodów (z powodu przerwy w działaniu usługi), wzrostu kosztów zarządzania incydentem, utraty reputacji, a także wzrostu percepcji ryzyka inwestorskiego — co czyni je istotnymi również w perspektywie wartości rynkowej przedsiębiorstw.

Wycieki danych

Wycieki danych to incydenty polegające na uzyskaniu przez osoby nieuprawnione dostępu do poufnych informacji, takich jak dane osobowe klientów, hasła, numery kart płatniczych czy tajemnice handlowe. Są one jednym z najpoważniejszych zagrożeń w cyberprzestrzeni, ponieważ dotyczą zarówno przedsiębiorstw, instytucji publicznych, jak i osób prywatnych. Wycieki danych mogą wynikać z różnorodnych przyczyn, w tym ataków hakerskich, błędów ludzkich, a nawet celowego działania osób wewnątrz organizacji.[34] Według raportu IBM, średni koszt jednego wycieku danych w 2021 roku wyniósł 4,35 miliona dolarów, co podkreśla skalę strat, jakie mogą ponosić firmy dotknięte takimi incydentami.[35]

Sztuczna inteligencja (*Artificial Intelligence* – AI) w działaniach cyberprzestępców

---

[32] Su Y., *A Comprehensive Survey of Distributed Denial of Service (DDoS) Attacks and Defenses*, *Electronics*, vol. 13(4), 2024, art. 807. DOI: 10.3390/electronics13040807.

[33] Raport z incydentu – GitHub: https://github.blog/news-insights/company-news/ddos-incident-report/ dostęp: 01.03.2025

[34] A. Von Solms, R. Von Solms, *Information Security Governance*, Springer, 2018, s. 112.

[35] M. Kowalski, „Rekordowo wysokie koszty naruszeń danych – raport IBM", „Computerworld Polska", 2021, dostęp: https://www.computerworld.pl/article/2502465/raport-ibm-rekordowo-wysokie-koszty-naruszen-danych.html, [dostęp: 20.11.2024].

Sztuczna inteligencja (Artificial Intelligence, AI) staje się coraz częściej wykorzystywana przez sprawców cyberprzestępstw, co zmienia charakter i skalę zagrożeń w cyberprzestrzeni. Generatywne modele językowe i sieci neuronowe umożliwiają automatyczne tworzenie wysoko realistycznych treści (tekstu, mowy i obrazu), które znacząco podnoszą skuteczność ataków socjotechnicznych — w tym phishingu ukierunkowanego (spear-phishing) oraz kampanii opartych na deepfake'ach[36]. Dzięki AI atakujący mogą:

- generować spersonalizowane, gramatycznie poprawne i naturalne e-maile w dużej skali;
- tworzyć wiarygodne nagrania głosowe i wideo (deepfake), np. w celu spoofingu menedżerów finansowych;
- automatyzować poszukiwanie luk i generować złośliwy kod adaptacyjny (polymorphic/AI-driven malware), który zmienia sygnaturę, aby unikać wykrycia.

Konsekwencje praktyczne zastosowania AI należy rozpatrywać dwojako. Po pierwsze — zwiększa się skuteczność ataków: tradycyjne heurystyki wykrywania phishingu (błędy językowe, nietypowe frazy) stają się mniej użyteczne, ponieważ generatory tekstu tworzą komunikaty o jakości porównywalnej z materiałami marketingowymi czy oficjalnymi komunikatami instytucji. Po drugie — obniżają się bariery wejścia dla mniej zaawansowanych przestępców: narzędzia AI pozwalają na szybkie przygotowanie przekonujących kampanii bez potrzeby dużych umiejętności programistycznych. Takie zjawiska podkreślają zarówno raporty branżowe, jak i analizy naukowe. Z punktu widzenia wykrywania i obrony, pojawienie się AI-generowanych ataków stawia nowe wyzwania: systemy oparte na statycznych regułach i sygnaturach muszą być uzupełnione o modele analizy behawioralnej, metryki „perplexity/burstiness" czy detektory AI-generowanych treści. Jednocześnie obie strony — obrona i atak — zaczynają wykorzystywać AI, co tworzy swoisty wyścig zbrojeń w obszarze modeli generatywnych i systemów detekcji. Badania empiryczne pokazują, że detektory oparte na cechach stylistycznych i modelach uczenia maszynowego mogą wykrywać AI-generowane

[36] S. Mirsky, W. Lee, The Emerging Threat of Deepfakes: How to Identify and Combat AI-Generated Deception, Proceedings of the ACM Conference on Information Systems Security (ACM SIGSAC), 2023, DOI: 10.1145/3584202.3584300

.

wiadomości, lecz ich skuteczność spada wobec modeli nowszej generacji i przy braku odpowiednio dużych, zróżnicowanych zbiorów treningowych[37] .

Ataki oparte na socjotechnice

Socjotechnika stanowi fundament wielu współczesnych cyberataków, wykorzystując manipulację psychologiczną ofiar w celu skłonienia ich do ujawnienia poufnych informacji, przekazania danych uwierzytelniających lub podjęcia działań umożliwiających przestępcom uzyskanie dostępu do systemów informatycznych. W przypadku ataków takich jak phishing, stosowane są fałszywe wiadomości e-mail lub strony internetowe, które imitują zaufane podmioty, aby nakłonić użytkownika do podania danych logowania lub pobrania złośliwego oprogramowania[38]. Wśród bardziej zaawansowanych form socjotechniki wyróżnia się również vishing (oszustwa telefoniczne oparte na podszywaniu się pod przedstawicieli banków lub instytucji publicznych) oraz smishing (atak z wykorzystaniem wiadomości SMS zawierających złośliwe linki lub fałszywe komunikaty o płatnościach, przesyłkach bądź blokadach konta). W literaturze przedmiotu podkreśla się, że skuteczność ataków socjotechnicznych wzrasta dzięki zastosowaniu personalizacji komunikatów – przestępcy analizują dane ofiar dostępne w Internecie, co pozwala na tworzenie przekazów dopasowanych do ich profilu i zwiększa prawdopodobieństwo sukcesu ataku. Badania empiryczne dowodzą, że kluczowym czynnikiem umożliwiającym powodzenie takich incydentów jest niedostateczne przygotowanie i brak szkoleń personelu w zakresie rozpoznawania i reagowania na potencjalne zagrożenia socjotechniczne. Jak wskazują autorzy licznych analiz, nawet najbardziej zaawansowane systemy zabezpieczeń nie są w stanie skutecznie przeciwdziałać manipulacji człowiekiem, jeśli brakuje odpowiednich procedur edukacyjnych i świadomości zagrożeń wśród pracowników[39].

---

[37] C. Eze, L. Shamir, Analysis and Prevention of AI-Based Phishing Email Attacks, IEEE Access, vol. 12, 2024, s. 31745–31759, DOI: 10.1109/ACCESS.2024.3390213

.

[38] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, *The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies*, *Computers & Security*, vol. 66, 2017, s. 40–51. DOI: 10.1016/j.cose.2017.01.004

[39] J. Ferreira, P. Ribeiro, T. Pereira, *Vishing and Smishing Threats: A Comparative Review of Methods and Mitigation Techniques*, *Journal of Information Security and Applications*, vol. 70, 2023, art. 103517. DOI: 10.1016/j.jisa.2023.103517.

Każdy z opisanych typów ataków stanowi poważne zagrożenie dla funkcjonowania współczesnych organizacji – zarówno ze względu na bezpośrednie straty finansowe, jak i konsekwencje reputacyjne. Zrozumienie ich mechanizmów oraz wdrażanie skutecznych programów prewencji, szkoleniowych i technologicznych jest kluczowe dla minimalizacji ryzyka. W dalszych częściach pracy przedstawiono analizę gospodarczych skutków tych ataków oraz strategii ograniczania ich wpływu na działalność przedsiębiorstw

3. Ewolucja technologii cyberbezpieczeństwa

Dynamiczny rozwój technologii cyfrowych zapoczątkowany w drugiej połowie XX w. prowadzi do ewolucji obszaru cyberbezpieczeństwa, która odzwierciedla zmieniające się potrzeby organizacji oraz wzrost wyrafinowania ataków cybernetycznych. Pierwotna ochrona danych, systemów i sieci ograniczona była do najprostszych metod, takich jak zapobieganie uzyskania dostępu czy antywirusy, natomiast obecnie obejmuje zaawansowane rozwiązania, które integrują sztuczną inteligencję, uczenie maszynowe oraz globalne standardy zarządzania ryzykiem. Historia rozwoju i zmian w technologii cyberbezpieczeństwa pokazuje, w jaki sposób zmieniały się narzędzia i procedury, który były stosowane w odpowiedzi na zwiększające się zagrożenia, a także jak ważną rolę odegrały regulacje prawne oraz międzynarodowe standardy.

Miniaturyzacja procesorów i innych komponentów elektronicznych, prowadząca do powstania komputerów osobistych (PC) zaowocowała w lata 70. i 80. XX w. implementacją technologii informatycznych w dużych podmiotach gospodarczych. Brak istnienia w tamtych czasach globalnej sieci Internetu powodował, że cyberzagrożenia koncentrowały się na manipulacjach pojedynczymi urządzeniami. Dlatego też pierwszymi reakcjami na tego typu problemy były implementacje programów antywirusowych, czy wprowadzenie systemów kontroli dostępu do jednostek komputerowych[40]. Pomimo swojej prostoty, technologie te zapoczątkowały rozwój bardziej zaawansowanych metod ochrony. Przełom lat 80. i 90. przyniósł rozkwit Internetu, który jednoznacznie, z uwagi na wzrost możliwych zagrożeń, stał

[40] Yost, J. R. (2015). Computer Security [Guest editors' introduction]. IEEE Annals of the History of Computing, 37(2), 6–7. https://doi.org/10.1109/MAHC.2015.33

się katalizatorem zmian w cyberbezpieczeństwie. W tym czasie cyberprzestępczość nabrała bardziej zorganizowanego charakteru, a ataki zaczęły obejmować całe sieci komputerowe. Dlatego niezbędne stało się wynalezienie sposób będących odpowiedzią na nowe wyzwania, którym było wprowadzenie zapór sieciowych (firewalle), które dzięki zaprogramowanym regułom miały za zadanie monitorowanie i filtrowanie ruchu. Sama technologia firewall także ewoluowała. Pierwsze generacje były stosunkowo proste – bazowały na analizie adresów IP i portów – jednak stanowiły kluczowy krok w kierunku bardziej zaawansowanej ochrony. Rozwiązania te były jednak niewystarczające w obliczu coraz bardziej skomplikowanych ataków, takich jak DDoS, które zaczęły dominować w latach 90[41]. W odpowiedzi na zmieniające się i gwałtownie rosnące zagrożenia, w końcu XX wieku rozwinięto systemy typu IDS (*Intrusion Detection Systems*) i IPS (*Intrusion Prevention Systems*), które nie tylko bazowały na prostych regułach, ale były w stanie analizować ruch sieciowy w czasie rzeczywistym. IDS służyły do wykrywania potencjalnie niebezpiecznych działań, natomiast IPS pozwalały na ich natychmiastowe blokowanie[42]. Technologie te stały się fundamentem ochrony sieci organizacji o kluczowym znaczeniu, takich jak infrastruktura krytyczna czy instytucje finansowe. Należy zaznaczyć, że równolegle rozwijały się także technologie szyfrowania danych. Początkowe algorytmy, takie jak DES, szybko zostały zastąpione przez bardziej zaawansowane standardy, takie jak na przykład AES (*Advanced Encryption Standard*), które oferowały wyższy poziom ochrony i były w stanie sprostać rosnącym wymaganiom w zakresie poufności informacji. Szczególną rolę i znaczenie szyfrowania danych można wskazać w transakcjach finansowych oraz komunikacji online, a protokoły SSL/TLS[43] stały się

[41] . Liang, Y. Kim, *Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall*, [w:], *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, IEEE, Las Vegas, 26–29 stycznia 2022, DOI: 10.1109/CCWC54503.2022.9720435, [dostęp: 26 listopada 2024]

[42] Karimi, A., Niyaz, Q., Sun, W., Javaid, A., & Devabhaktuni, V. (2016). Distributed network traffic feature extraction for a real-time IDS. *2016 IEEE International Conference on Electro Information Technology (EIT)*, 0522-0526. https://doi.org/10.1109/EIT.2016.7535295.

[43] SSL (Secure Sockets Layer) i **TLS (Transport Layer Security)** to protokoły kryptograficzne służące do zabezpieczania komunikacji w internecie.

- **SSL** – to starsza wersja protokołu, która była powszechnie stosowana do szyfrowania połączeń między przeglądarkami a serwerami.
- **TLS** – to jego ulepszona wersja, zapewniająca większe bezpieczeństwo i lepszą wydajność. TLS zastąpił SSL, a jego najnowsza wersja to **TLS 1.3**.

podstawą ochrony w handlu elektronicznym[44]. W XXI wieku transformacja cyfrowa napędzona rozwojem globalnej sieci i wzrostem liczby urządzeń podłączonych do Internetu skutkowała pojawieniem się Internetu rzeczy (IoT) oraz coraz większej popularności usług chmurowych[45]. Spowodowane było to nowymi wyzwaniami dla bezpieczeństwa danych i systemów komputerowych. Zaczęto stosować coraz bardziej wyrafinowane techniki ochrony jak na przykład segmentację sieci, która polega na podziale infrastruktury na mniejsze, izolowane segmenty. Dzięki temu możliwe było ograniczenie rozprzestrzeniania się zagrożeń w przypadku naruszenia bezpieczeństwa jednego z segmentów.

Kolejnym ważnym krokiem w ewolucji cyberbezpieczeństwa było zastosowanie technologii opartych na sztucznej inteligencji i uczeniu maszynowym. Efektem czego było powstanie systemów SIEM (*Security Information and Event Management*) oraz EDR (*Endpoint Detection and Response*). Umożliwiają one analizę ogromnych liczby danych w czasie rzeczywistym, identyfikację wzorców charakterystycznych dla ataków oraz przewidywanie potencjalnych zagrożeń[46]. Zastosowanie technologii AI pozwoliło na znaczną automatyzację tych, co w sposób istotny zwiększyło skuteczność działań ochronnych.

Kolejnym przykładem automatyzacji procesów są systemy SOAR (*Security Orchestration, Automation, and Response*), które integrują dane z różnych źródeł, takich jak logi systemowe, analiza ruchu sieciowego czy wyniki testów penetracyjnych. SOAR umożliwia szybkie podejmowanie decyzji i automatyczne wdrażanie środków zaradczych, co przyczynia się do minimalizacji skutków ataków[47]. Kolejny obszar, które przechodzi dynamiczny rozwój obejmuje technologie ochrony danych osobowych. Należy do nich zaliczyć narzędzia klasy DLP (*Data Loss Prevention*), które umożliwiają monitorowanie i zapobieganie nieautoryzowanemu przesyłowi danych poza organizację[48]. Takie rozwiązania stały się

[44] Pandya, D., Narayan, K., Thakkar, S., Madhekar, T., & Thakare, B. (2015). Brief History of Encryption. *International Journal of Computer Applications*, 131, 28-31. https://doi.org/10.5120/ijca2015907390.
[45] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431–440. https://doi.org/10.1016/J.BUSHOR.2015.03.008
[46] Inns, J. (2014). The evolution and application of SIEM systems. *Network Security, 2014*(9), 16-17. https://doi.org/10.1016/S1353-4858(14)70051-0
[47] Bridges, R., Rice, A. E., Oesch, S., Nichols, J. A., Watson, C., & Spakes, K. D. (2022). Testing SOAR Tools in Use. *ArXiv*. https://doi.org/10.48550/arXiv.2208.06075
[48] Takebayashi, T., Tsuda, H., Hasebe, T., & Masuoka, R. (2010). Data Loss Prevention Technologies. *Fujitsu Scientific & Technical Journal, 46*, 47-55.

szczególnie istotne po wprowadzeniu na poziomie krajowym regulacji w zakresie ochrony danych osobowych.

Przyszłość cyberbezpieczeństwa to dalsze rozwijanie technologii opartych na sztucznej inteligencji oraz automatyzacji procesów. W praktyce coraz częściej spotyka się organizacje, które korzystają z systemów integrujących dane z różnych źródeł, co pozwalają na predykcyjną analizę zagrożeń i minimalizację ryzyka[49]. Jednocześnie rosnąca liczba regulacji oraz zmieniające się przepisy międzynarodowe będą wymuszać na firmach dalsze inwestycje w zaawansowane technologie ochrony danych i infrastrukturę IT. Podsumowując, ewolucja technologii cyberbezpieczeństwa odzwierciedla nieustanną walkę między zatrudnionymi w organizacjach specjalistami ds. cyberbezpieczeństwa, a cyberprzestępcami. Rozwój narzędzi ochrony miał charakter responsywny i umożliwił lepsze zabezpieczenie zasobów cyfrowych. Jednak w miarę jak pojawiają się nowe zagrożenia, potrzeba ciągłego doskonalenia technologii i strategii cyberbezpieczeństwa staje się coraz silniejsza. W erze cyfrowej, gdzie dane stanowią jeden z najcenniejszych zasobów, cyberbezpieczeństwo jest nie tylko kwestią techniczną, ale także kluczowym elementem zarządzania ryzykiem i budowania przewagi konkurencyjnej.

4. Koszty cyberataków dla gospodarki i przedsiębiorstw

Ccyberataki generują coraz większe koszty, które dotykają zarówno indywidualnych podmiotów, jak i także całe gospodarki. W wyniku ataków przedsiębiorstwa i inne instytucje ponoszą straty finansowe, doświadczają zakłóceń działalności operacyjnej, utraty reputacji wśród konsumentów, a także są zmuszone do ponoszenia wydatków na odbudowę systemów oraz spełniania wymogów regulacji prawnych. Biorąc pod uwagę perspektywę makroekonomiczną, koszty te wpływają na wzrost czynnika ryzyka inwestycyjnego, zmniejszenie produktywności oraz spowolnienie tempa innowacji[50].

Jednym z najbardziej widocznych skutków cyberataków są bezpośrednie straty finansowe. Mogą one wynikać z konieczności zapłaty okupu w przypadku ataków *ransomware*,

[49] Ramakrishnan, R. (2023). The Future of Cybersecurity and Its Potential Threats. *International Journal for Research in Applied Science and Engineering Technology*. https://doi.org/10.22214/ijraset.2023.54603
[50] M. F. Franco, F. Künzler, J. von der Assen, C. Feng, B. Stiller, „RCVaR: An economic approach to estimate cyberattacks costs using data from industry reports", „Computers & Security", 2024, vol. 103737

takich jak atak na Colonial Pipeline, gdzie okup wyniósł 4,4 miliona dolarów.[51] Do tego należy doliczyć koszty przerw w działalności, które w przypadku dużych firm mogą wynosić miliony dolarów dziennie. Przykładowo, według raportu IBM, średni koszt jednego wycieku danych wyniósł w 2022 roku 4,35 miliona dolarów, co obejmuje zarówno odzyskiwanie danych, jak i utratę przychodów[52]. Cyberataki często powodują znaczne zakłócenia w działalności operacyjnej przedsiębiorstw. Na przykład zainfekowanie systemów przez *ransomware* lub ataki DDoS może na długi czas uniemożliwić realizację podstawowych procesów biznesowych organizacji, takich jak przetwarzanie zamówień czy komunikacja z klientami. Przykładem może być atak na sieć szpitali w Wielkiej Brytanii w 2017 roku (WannaCry), który doprowadził do odwołania tysięcy operacji oraz wizyt lekarskich, co dodatkowo zwiększyło koszty związane z naprawą systemów i rekompensatą dla pacjentów[53].

Innym negatywnym aspektem cyberataków są koszty reputacyjne. Utrata zaufania klientów to jedno z najbardziej długotrwałych następstw cyberataków. Wycieki danych osobowych klientów, jak w przypadku ataku na firmę Equifax w 2017 roku, mogą prowadzić do odpływu klientów z firm oraz trudności w pozyskiwaniu nowych kontraktów[54]. Koszty te są trudne do oszacowania, ale można do nich zaliczyć m.in. wydatki na kampanie odbudowujące wizerunek, takie jak programy monitorowania kredytowego dla poszkodowanych klientów czy dodatkowe inwestycje w ochronę danych.

Kolejna rodzaj kosztów wiąże się z wdrażanie regulacji dotyczących cyberbezpieczeństwa, obejmującymi zarówno jednorazowe wydatki na dostosowanie systemów, jak i bieżące koszty utrzymania zgodności z przepisami. Obciążenia te wynikają z konieczności inwestycji w nowoczesne technologie zabezpieczające, przeprowadzania audytów, szkoleń personelu oraz zatrudnienia specjalistów ds. cyberbezpieczeństwa. Dodatkowo, firmy muszą uwzględnić potencjalne kary finansowe za nieprzestrzeganie

[51] PAP, „Amerykańskie służby odzyskały część okupu zapłaconego hakerom", „TVN24 Świat", 2021, dostęp: https://tvn24.pl/swiat/usa-amerykanskie-sluzby-odzyskuja-czesc-okupu-oplaconego-hakerom-przez-colonial-pipeline-st5115065

[52] IBM, „Consumers Pay the Price as Data Breach Costs Reach All-Time High", „IBM Newsroom", 2022, dostęp: https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time-High, [dostęp: 20.11.2024].

[53] National Audit Office, „Investigation: WannaCry cyber attack and the NHS", „Value for Money Report", 27 października 2017, dostęp: https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/, [dostęp: 20.11.2024]

[54] C. Ikezuruora, „Beyond Headlines: Case Study - The Equifax Data Breach and Lessons Learned", 1 lutego 2024, dostęp: https://www.example.com/beyond-headlines-equifax-data-breach, [dostęp: 20.11.2024].

regulacji, co może znacząco wpłynąć na ich budżety. W kontekście dyrektywy NIS2[55], która ma na celu wzmocnienie poziomu cyberbezpieczeństwa w Unii Europejskiej, przewiduje się znaczne obciążenia finansowe dla przedsiębiorstw. Według autorów raportu pn. *„Assessing the Economic Impact of EU Initiatives on Cybersecurity"*, koszt roczny wdrożenia w Unii Europejskiej nowych regulacji dotyczących cyberbezpieczeństwa przez przedsiębiorstwa to ok. 31,2 mld euro[56]. Zgodnie z danymi zawartymi w raporcie, przewidywane koszty obejmują m.in. wydatki na zatrudnienie specjalistów ds. cyberbezpieczeństwa, zakup oprogramowania oraz instalację sprzętu niezbędnego do spełnienia wymogów dyrektywy. Należy zwrócić uwagę, że przepisy dotyczące cyberbezpieczeństwa nakładają koszty nie tylko na podmioty rynkowe, ale także na organy odpowiedzialne za wdrażanie i monitorowanie przepisów. Na przykład w Polsce wdrożenie dyrektywy NIS będzie wymagało utworzenia Sektorowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego(CSIRT) oraz regionalnych centrów cyberbezpieczeństwa[57]. Koszty wdrożenia nowych przepisów dla podmiotów nieobjętych wcześniej dyrektywą NIS będą znacznie wyższe niż dla tych, które miały czas wdrożyć poprzednio obowiązujące wymogi. Implementacja dyrektywy NIS2[58] wiąże się z istotnymi kosztami dla przedsiębiorstw, zarówno w Polsce, jak i w całej Unii Europejskiej, jednakże inwestycje te są niezbędne dla zapewnienia odpowiedniego poziomu cyberbezpieczeństwa oraz ochrony przed rosnącym zagrożeniem cyberataków.

Na poziomie krajowym cyberataki mogą prowadzić do zmniejszenia produktywności, spowolnienia wzrostu gospodarczego oraz wzrostu ryzyka inwestycyjnego. Przykładem może być wpływ zakłóceń w sektorze energetycznym, który ma kluczowe znaczenie dla

---

[55] Parlament Europejski i Rada Unii Europejskiej, *Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (Dyrektywa NIS2)*, Dz. Urz. UE L 333 z 27 grudnia 2022 r., s. 80–152.

[56] Frontier Economics, „Assessing the Economic Cost of EU Initiatives on Cybersecurity: The Impact of NIS2", 12 lipca 2023, dostęp: https://www.frontier-economics.com/media/a.pdf, [dostęp: 20.11.2024].

[57] Ministerstwo Cyfryzacji, „Krajowy system cyberbezpieczeństwa – zadania i cele", „Gov.pl", dostęp: https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-, [dostęp: 20.11.2024].

[58] Parlament Europejski i Rada Unii Europejskiej, *Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (NIS2)*, Dz.U. UE L 333 z 27.12.2022, s. 80–152.

funkcjonowania innych gałęzi gospodarki[59]. Według prognoz ekspertów, globalne koszty związane z cyberprzestępczością mają osiągnąć 10,5 biliona dolarów rocznie do 2025 roku, co stanowi ogromne obciążenie dla gospodarek rozwiniętych i rozwijających[60]. Szczególnie narażony na skutki cyberataków jest sektor małych i średnich przedsiębiorstw (MŚP) ze względu na ograniczone zasoby finansowe i technologiczne, które utrudniają wdrażanie zaawansowanych systemów bezpieczeństwa. Według raportu KPMG z 2023 roku, 66% firm w Polsce odnotowało przynajmniej jeden incydent związany z cyberbezpieczeństwem, co stanowi wzrost o 8% w porównaniu z rokiem poprzednim[61]. Dodatkowo, dane z raportu Związku Cyfrowa Polska wskazują, że w 2021 roku 64% polskich firm doświadczyło co najmniej jednego incydentu cyberbezpieczeństwa, co stanowi wzrost o 10% względem 2019 roku[62]. Statystyki te podkreślają rosnące zagrożenie dla MŚP w Polsce, które często dysponują ograniczonymi zasobami na inwestycje w zaawansowane systemy ochrony przed cyberzagrożeniami. Cyberataki mogą również wpływać na ograniczenie innowacyjności przedsiębiorstw, które muszą przekierowywać swoje zasoby na odbudowę i zabezpieczenie systemów, zamiast na rozwój nowych produktów czy usług[63]. Przykładem może być sektor technologiczny, gdzie opóźnienia w realizacji projektów badawczo-rozwojowych mogą skutkować utratą przewagi konkurencyjnej[64]. W dłuższej perspektywie takie przesunięcia wydatków mogą mieć negatywny wpływ na całe branże, ograniczając tempo ich rozwoju.

Podsumowując, koszty cyberataków mają wielowymiarowy charakter i wykraczają daleko poza bezpośrednie straty finansowe. Ich wpływ obejmuje aspekty operacyjne, regulacyjne, a także makroekonomiczne i społeczne. Zrozumienie tych kosztów jest kluczowe

---

[59] Avraam C., Ceferino L., Dvorkin Y., *Operational and Economy-Wide Impacts of Compound Cyberattacks and Extreme Weather Events on Electric Power Networks*, *arXiv preprint*, 2022, https://arxiv.org/abs/2209.04927 (dostęp: 24 października 2025).

[60] S. Morgan, „Cybercrime To Cost The World $10.5 Trillion Annually By 2025", „Cybercrime Magazine", 13 listopada 2020, dostęp: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/, [dostęp: 20.11.2024].

[61] KPMG, „Barometr cyberbezpieczeństwa 2023", 2023, dostęp: https://kpmg.com/pl/pl/home/insights/2024/02/barometr-cyberbezpieczenstwa-2024.html, [dostęp: 20.11.2024].

[62] Związek Cyfrowa Polska, „Raport o stanie cyberbezpieczeństwa polskich firm 2021", 2021, dostęp: https://cyfrowapolska.org/pl/raport_cyber2021/, [dostęp: 20.11.2024]

[63] Wang J., *Does cybersecurity risk stifle corporate innovation activities?*, *Journal of Corporate Finance*, vol. 76, 2024, s. 102212.

[64] Merck & Co., *Still reeling from cyber-attack, Merck warns some drug and vaccine production & R&D still recovering*, komunikat prasowy, 28 lipca 2017

dla opracowania skutecznych strategii ochrony, które minimalizują negatywne skutki dla przedsiębiorstw i gospodarki jako całości. W dalszych rozdziałach pracy przeanalizowane zostaną konkretne przypadki oraz metody zarządzania ryzykiem cyberbezpieczeństwa.

5. Wpływ cyberataków na zachowania konsumentów i zaufanie do f rm

Cyberataki wywierają ogromny wpływ na współczesne przedsiębiorstwa, a w szczególności na relacje z klientami i poziom zaufania konsumentów. W dobie cyfryzacji, w której dane osobowe stanowią cenny zasób strategiczny, każde naruszenie bezpieczeństwa może prowadzi do poważnych konsekwencji operacyjnych, wizerunkowych i finansowych. Fundamentem stabilnych relacji biznesowych jest często zaufanie konsumentów. Może ono zostać poważnie podważone, gdy organizacja nie jest w stanie zapewnić odpowiedniej ochrony danych. Badania wskazują, że aż 75% klientów rezygnuje z usług firm, które nie potrafiły skutecznie zabezpieczyć ich danych osobowych[65]. To znacząco wpływa na lojalność klientów, a w konsekwencji na przyszłe decyzje zakupowe i preferencje konsumentów. Należy zwrócić uwagę, że utrata zaufania do organizacji często ma długotrwałe konsekwencje, nie tylko dla podmiotu, ale i całego sektora w którym funkcjonuje[66].

Przykładem znaczących konsekwencji wizerunkowych cyberataków może być incydent z udziałem firmy Equifax w 2017 roku. W wyniku wycieku danych osobowych 147 milionów klientów doszło do masowego odpływu klientów i gwałtownego spadku zaufania do tej instytucji. Equifax przez wiele lat zmagał się z trudnościami w odbudowie swojej pozycji na rynku oraz z rosnącą niechęcią do współpracy ze strony konsumentów. Incydent ten stał się również punktem wyjścia do zmian regulacyjnych, które wymusiły na firmach bardziej rygorystyczne podejście do ochrony danych[67]. W takich przypadkach zarządzanie kryzysowe staje się nieodzownym elementem strategii organizacji. Kryzysy związane z naruszeniem bezpieczeństwa danych czy innymi zagrożeniami wizerunkowymi mogą pojawić się nagle i

[65] K. Pasławski, Konsumenci porzucają firmy, którym nie ufają ws. danych, [online], *Prawo.pl*, dostęp: 22 listopada 2024, https://www.prawo.pl/biznes/z-firmy-z-ktorej-wyciekly-dane-konsumenci-nie-chca-kupowac, [dostęp: 26 listopada 2024].
[66] H. Cavusoglu, B. Mishra, S. Raghunathan, The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers, „International Journal of Electronic Commerce", 2004, nr 2 (9), s. 69–104.
[67] C. Ikezuruora, *Beyond Headlines: Case Study - The Equifax Data Breach and Lessons Learned*, https://www.securitymagazine.com/articles/97944-beyond-headlines-case-study-the-equifax-data-breach-and-lessons-learned, [dostęp: 26 listopada 2024].

wymagać natychmiastowej reakcji. Dlatego jednym z kluczowych aspektów zarządzania w takich sytuacjach jest skuteczna komunikacja z konsumentami, która pozwala ograniczyć negatywne skutki zdarzenia. Istotnym elementem jest transparentność działań, jak również niezwłoczne wdrażanie środków naprawczych[68]. Powoduje to nie tylko wzmacnianie wiarygodności przedsiębiorstwa, ale również stanowi fundament odbudowy zaufania wśród dotychczasowych klientów. Znaczenie transparentności w zarządzaniu kryzysowym obejmuje nie tylko ujawnienie szczegółów incydentu, ale również, co niezwykle istotne, wyjaśnienie kroków, które zostały podjęte, aby zabezpieczyć dane klientów. Badania wskazują, że konsumenci są bardziej skłonni „wybaczyć" organizacjom, które otwarcie informują o swoich problemach i podejmują działania naprawcze[69]. Natomiast brak transparentności może działać przeciwnie i prowadzić do eskalacji problemów wizerunkowych. Długofalowe konsekwencje braku odpowiedniego zarządzania kryzysowego to wzrost kosztów pozyskiwania nowych klientów, trudności w utrzymaniu obecnych oraz utrata przewagi konkurencyjnej na rynku[70].

Wiele podmiotów gospodarczych organizuje akcje edukacyjne dla klientów jako element strategii zarządzania skutkami cyberataków. Organizacje coraz częściej decydują się na wdrożenie programów, których celem jest zwiększenie świadomości konsumentów w zakresie higieny cyfrowej. Przykłady takich inicjatyw mogą obejmować np. szkolenia dotyczące rozpoznawania prób phishingowych, stosowania silnych haseł czy unikania niebezpiecznych działań w sieci. Programy te, oprócz minimalizacji szans na wystąpienie potencjalnych incydentów, mają również na celu wzmocnienie więzi między klientem, a podmiotem gospodarczym[71]. Przykładem skutecznej edukacji konsumentów mogą być działania podejmowane przez instytucje bankowe, które oferują swoim klientom darmowe narzędzia monitorujące aktywność na kontach oraz szkolenia w zakresie zabezpieczania transakcji *online*. Takie działania w Polsce podejmuje m.in. PKO, który regularnie prowadzi kampanie edukacyjne i komunikacyjne w zakresie cyberbezpieczeństwa, dostosowując je do aktualnych zagrożeń. Doradcy i eksperci banku spotykają się stacjonarnie z klientami, aby

[68] K. Raissouni, Z. Errabih, S. Bourekkadi, *Cyber-attack crisis management in the context of energy companies*, [w:], *E3S Web of Conferences brakuje roku*

[69] Martin K. D., Borah A., Palmatier R. W., *A Strong Privacy Policy Can Save Your Company Millions*, [w:] *Harvard Business Review*, 15 II 2018.

[70] T. Aoyama, A. Sato, G. Lisi, *On the Importance of Agility, Transparency, and Positive Reinforcement in Cyber Incident Crisis Communication*, [online], 23 września 2019

[71] P. Choong, E. Hutton, P. S. Richardson, *Protecting the Brand: Evaluating the Cost of Security Breach from a Marketer's Perspective*, [w:], *Journal of Marketing Development and Competitiveness*, 1 marca 2017

dostarczyć im wiedzę na temat działania oszustów i metod manipulacji. Ponadto, bank informuje o aktualnych zagrożeniach oraz zasadach cyberbezpieczeństwa na swoich stronach internetowych, w serwisie iPKO, aplikacji IKO oraz w mediach społecznościowych[72].

Podsumowując, cyberataki mają wielowymiarowy wpływ na zachowania konsumentów i ich zaufanie do firm. W dobie cyfrowej transformacji gospodarki, naruszenia bezpieczeństwa danych mogą prowadzić do poważnych konsekwencji operacyjnych, finansowych i reputacyjnych, które są odczuwalne zarówno przez same organizacje, jak i ich klientów. Skuteczne zarządzanie skutkami cyberataków wymaga od przedsiębiorstw kompleksowego i strategicznego podejścia, obejmującego transparentność komunikacji kryzysowej, systematyczną edukację klientów oraz regularne inwestycje w nowoczesne technologie ochrony danych. Firmy, które potrafią szybko i efektywnie reagować na incydenty cybernetyczne, nie tylko minimalizują ich bezpośrednie skutki finansowe i operacyjne, ale również mają szansę wzmocnić swoją reputację oraz zbudować głębsze relacje z klientami oparte na zaufaniu. Przykłady dużych instytucji finansowych, takich jak PKO Bank Polski wskazują na istotną rolę edukacji i świadomości w zakresie cyberbezpieczeństwa. Inicjatywy te, obejmujące narzędzia monitorowania aktywności na kontach oraz szeroko zakrojone kampanie informacyjne i szkoleniowe, pokazują, że aktywne zaangażowanie klientów w ochronę ich danych osobowych i finansowych stanowi istotny element strategii odpornościowej przedsiębiorstw. W obliczu rosnącego znaczenia technologii cyfrowych we wszystkich aspektach funkcjonowania rynku, zdolność firm do zarządzania ryzykiem cybernetycznym będzie coraz mocniej decydowała o ich przewadze konkurencyjnej oraz sukcesie biznesowym. Budowanie trwałego zaufania konsumentów wymaga nie tylko zapewnienia skutecznej ochrony danych, ale także transparentnego informowania klientów o działaniach podejmowanych w celu minimalizowania ryzyka. Ostatecznie, organizacje, które będą w stanie połączyć inwestycje w zaawansowane technologie z efektywną komunikacją oraz edukacją swoich klientów, zwiększą swoją odporność na cyberzagrożenia, jednocześnie wzmacniając swoją pozycję rynkową i reputację w perspektywie długoterminowej.

[72]PKO Bank Polski. Komuniakt medialny. https://media.pkobp.pl/376587-po-pierwsze-bezpieczenstwo-od-maja-nowy-regulamin-dla-klientow-pko-banku-polskiego data dostepu: 2025.03.12

ROZDZIAŁ II. RYNKI FINANSOWE I ICH PODATNOŚĆ NA CYBERATAKI

1. Charakterystyka rynków f nansowych

Rynek finansowy jest strukturą organizacyjną i instytucjonalną, na której dochodzi do zawierania transakcji kupna i sprzedaży instrumentów finansowych. Pełni on kluczową rolę w gospodarce, umożliwiając alokację kapitału oraz efektywną wymianę zasobów finansowych pomiędzy podmiotami posiadającymi ich nadwyżki a tymi, które zgłaszają zapotrzebowanie na dodatkowe środki finansowe[73]. Struktura rynków finansowych jest złożona i obejmuje różne segmenty, takie jak rynek kapitałowy, rynek pieniężny, rynek walutowy, rynek instrumentów pochodnych czy rynek kredytowy i depozytowy, a każdy z nich ma swoją specyfikę i funkcje w gospodarce. Segmenty te różnią się rodzajem instrumentów finansowych, które są na nich dostępne, rodzajem uczestników oraz sposobami dokonywania transakcji, co sprawia, że cała struktura rynków finansowych cechuje się wysoką dynamiką i zdolnością do dostosowywania się do zmieniających się potrzeb gospodarki[74].

Na *rynku kapitałowym* przedsiębiorstwa pozyskują kapitał m.in. poprzez emisję akcji i obligacji, umożliwiając inwestorom angażowanie środków w różnorodne projekty biznesowe. Z kolei *rynek pieniężny* zaspokaja krótkoterminowe potrzeby finansowe uczestników, oferując takie instrumenty jak bony skarbowe czy certyfikaty depozytowe. *Rynek walutowy* zapewnia wymianę różnych walut, co jest niezbędne w kontekście globalizacji i współpracy międzynarodowej, podczas gdy *rynek instrumentów pochodnych* pozwala na zarządzanie ryzykiem związanym z fluktuacjami cen, kursów walutowych czy stóp procentowych[75].

Współczesne rynki finansowe funkcjonują w środowisku dynamicznie zmieniającej się technologii, która nie tylko ułatwia zawieranie transakcji, ale również zwiększa ich podatność

[73] Prasad, S. (2020). Role of Financial Innovations in Economic Development. , 40, 133-136.
[74] Gwoździewicz, S., & Prokopowicz, D. (2017). The normative role of the central bank on the money market in Poland.
[75] Wieland, I., Kovács, L., & Savchenko, T. (2020). Conceptual study of the difference between the money market and the capital market. *Financial Markets, Institutions and Risks, 4*(1), 51–59. https://doi.org/10.21272/fmir.4(1).51-59.2020

na zagrożenia cyfrowe. Rozwój platform elektronicznych i systemów algorytmicznych przyczynił się do wzrostu efektywności operacyjnej oraz zmniejszenia kosztów transakcyjnych. Jednocześnie cyfryzacja spowodowała, że pojawiły się nowe ryzyka, takie jak np. ataki typu DDoS, kradzież danych czy manipulacje cenami aktywów za pomocą zautomatyzowanych narzędzi. Wraz z globalizacją i cyfryzacją instytucje finansowe muszą coraz bardziej inwestować w rozwój zaawansowanych technologii bezpieczeństwa, takich jak np. sztuczna inteligencja czy *blockchain*, aby zapewnić ochronę przed coraz bardziej wyrafinowanymi zagrożeniami.[76]

Ważnym elementem funkcjonowania rynków finansowych są regulacje prawne, które mają na celu ochronę interesów uczestników oraz zapewnienie stabilności całego systemu. Wprowadzenie dyrektyw takich jak MiFID II[77] czy NIS2[78] zwiększyło zakres obowiązków nakładanych na instytucje finansowe, w tym konieczność stosowania odpowiednich zabezpieczeń informatycznych oraz raportowania incydentów bezpieczeństwa. Regulacje te mają na celu zwiększenie przejrzystości rynku oraz przeciwdziałanie manipulacjom, co w konsekwencji przyczynia się do budowy zaufania uczestników do całego systemu finansowego[79]. Rynki finansowe są również istotnym mechanizmem w kontekście globalnej alokacji kapitału, co potwierdzają badania wskazujące, że ich efektywność jest kluczowa dla wzrostu gospodarczego i rozwoju przedsiębiorczości. Zjawiska takie jak rozwój giełd papierów wartościowych czy wzrost popularności instrumentów pochodnych pozwalają na lepsze zarządzanie ryzykiem przez inwestorów oraz większe możliwości finansowania projektów inwestycyjnych. Jednakże w coraz bardziej skomplikowanym otoczeniu technologicznym i regulacyjnym, wyzwania związane z cyberbezpieczeństwem i automatyzacją handlu stają się coraz bardziej istotne[80].

---

[76] Babych, O. (2023). Digitalisation of Financial Markets, Current Issues, and Challenges. *State and Regions. Series: Economics and Business*. DOI: 10.32782/1814-1161/2023-3-1

[77] Parlament Europejski i Rada Unii Europejskiej, *Dyrektywa 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych (MiFID II)*, Dz.U. UE L 173 z 12.6.2014, s. 349–496.

[78] Parlament Europejski i Rada Unii Europejskiej, *Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (NIS2)*, Dz.U. UE L 333 z 27.12.2022, s. 80–152.

[79] Yeoh, P. (2018). MiFID II Opportunities and Regulatory Challenges. *Business Law Review*, 39(3), 111–123. https://doi.org/10.54648/bula2018022

[80] Gontareva, I., Chorna, M., Pawliszczy, D., Barna, M., Dorokhov, O., & Osinska, O. (2018). Features of the Entrepreneurship Development in Digital Economy. *TEM Journal, 7*(4), 857–868. DOI: 10.18421/tem74-19

Cyberzagrożenia, które stanowią obecnie jedno z największych wyzwań dla rynków finansowych, obejmują zarówno zagrożenia operacyjne, jak i zagrożenia systemowe. Zagrożenia operacyjne związane są przede wszystkim z możliwością zakłócenia bieżącej działalności instytucji finansowych na poziomie technologicznym i operacyjnym. Do tej kategorii zaliczają się między innymi ataki typu ransomware, DDoS, czy phishing, których bezpośrednimi konsekwencjami są utrudnienia lub całkowita przerwa w świadczeniu usług, błędy transakcyjne, czy utrata danych klientów. Z kolei zagrożenia systemowe mają charakter bardziej złożony i obejmują sytuacje, w których incydenty cybernetyczne mogą prowadzić do zakłóceń funkcjonowania całych segmentów rynku finansowego lub nawet systemu finansowego jako całości. Przykładem takich zagrożeń mogą być zaawansowane ataki na infrastrukturę krytyczną, skoordynowane manipulacje cenami instrumentów finansowych, czy ataki na globalne systemy rozliczeniowe, co może wywołać efekt domina i prowadzić do destabilizacji szeroko rozumianego systemu finansowego.

Ataki hakerskie na giełdy czy instytucje finansowe mogą prowadzić do poważnych zakłóceń, takich jak zawieszenie obrotu, manipulacje cenami czy utrata danych klientów. Ponadto automatyzacja handlu niesie za sobą ryzyko błędów systemowych, które mogą prowadzić do destabilizacji cen aktywów lub nawet poważnych krachów rynkowych. Przykłady takie jak tzw. *flash crash*, czyli gwałtowne spadki cen wywołane błędami w algorytmach, pokazują, jak dużą wagę należy przykładać do kontroli systemów technologicznych. W kontekście przyszłych wyzwań istotne jest także uwzględnienie potencjału, jaki niesie ze sobą sztuczna inteligencja w analizie danych rynkowych, prognozowaniu trendów czy zarządzaniu ryzykiem. Jednocześnie należy pamiętać, że rozwój tych technologii wymaga odpowiednich ram regulacyjnych oraz zaawansowanego systemu monitorowania ich wdrożenia, aby uniknąć ryzyk związanych z ich nadużyciami lub niewłaściwym zastosowaniem. Postęp technologiczny, mimo swoich zalet, wymaga zatem ciągłej współpracy między instytucjami finansowymi, regulatorami oraz uczestnikami rynku w celu utrzymania równowagi między innowacyjnością a bezpieczeństwem[81].

[81] Deshpande, A. S. (2024). Cybersecurity in Financial Services: Addressing AI-Related Threats and Vulnerabilities. *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*, 1, 1-6. https://doi.org/10.1109/ICKECS61492.2024.10616498

Podsumowując, rynki finansowe są niezwykle złożonym mechanizmem, który pełni kluczową funkcję w gospodarce światowej. Ich efektywne funkcjonowanie zależy od wielu czynników, takich jak m.in. innowacyjność technologiczna, regulacje prawne czy zdolność uczestników do adaptacji w zmieniających się warunkach. Jednak w obliczu rosnących zagrożeń cyfrowych i dynamicznej globalizacji konieczne jest dalsze doskonalenie mechanizmów zabezpieczających oraz rozwijanie strategii zarządzania ryzykiem, aby zapewnić ich stabilność i odporność na nowe wyzwania.

2. Segmenty rynków f nansowych

Rynek finansowy stanowi fundamentalny element systemu gospodarczego, pełniąc kluczowe funkcje w zakresie alokacji kapitału oraz zapewnienia płynności finansowej. Współczesny rynek finansowy można podzielić na kilka głównych segmentów, z których każdy odgrywa istotną rolę w procesie finansowania przedsiębiorstw, gospodarstw domowych oraz instytucji publicznych[82]. Pierwszym z nich jest rynek pieniężny, obejmujący krótkoterminowe instrumenty finansowe, takie jak bony skarbowe, certyfikaty depozytowe czy weksle handlowe, które umożliwiają podmiotom gospodarczym zarządzanie płynnością oraz finansowanie bieżącej działalności operacyjnej. Charakteryzuje się on niskim ryzykiem inwestycyjnym oraz wysoką płynnością aktywów, odgrywając kluczową rolę w polityce banków centralnych poprzez kontrolę podaży pieniądza i stabilizację systemu finansowego[83]. Kolejnym segmentem jest rynek kapitałowy, który umożliwia długoterminowe finansowanie poprzez emisję instrumentów takich jak akcje, obligacje i inne papiery wartościowe. Dzieli się on na rynek pierwotny, gdzie nowe papiery wartościowe są emitowane, a kapitał trafia bezpośrednio do emitenta, oraz rynek wtórny, na którym inwestorzy mogą handlować już istniejącymi instrumentami finansowymi. Efektywne funkcjonowanie rynku kapitałowego jest niezbędne dla wzrostu gospodarczego, gdyż umożliwia firmom pozyskiwanie środków na rozwój i

[82] Mykhalchynets, H. (2023). FINANCIAL MARKET AS A BASIS FOR EVALUATING TRANSFORMATION PROCESSES AND FORECASTING ITS EFFICIENCY THROUGH PERFORMANCE: CLASSIFICATION AND FORMS. *Herald of Khmelnytskyi National University. Economic sciences*. https://doi.org/10.31891/2307-5740-2023-314-1-12.

[83] Eisenschmidt, J., Kedan, D., & Tietz, R. (2018). Measuring fragmentation in the euro area unsecured overnight interbank money market. , 5.

innowacje[84]. Rynek walutowy, znany również jako Forex, to globalna platforma obrotu walutami, pozwalająca na wymianę jednej waluty na inną. Jego głównym celem jest zarządzanie ryzykiem kursowym oraz zapewnienie płynności transakcji międzynarodowych. Uczestnikami tego rynku są banki centralne, banki komercyjne, fundusze hedgingowe, korporacje międzynarodowe oraz inwestorzy indywidualni. Kluczowe instrumenty obejmują transakcje spot, polegające na natychmiastowej wymianie walut, kontrakty forward, umożliwiające zabezpieczenie przed zmianami kursów walutowych, oraz opcje walutowe, pozwalające na spekulację i ograniczanie ryzyka kursowego[85]. Rynek terminowy, obejmujący instrumenty pochodne takie jak kontrakty terminowe, opcje oraz inne instrumenty zależne od wartości aktywów bazowych (np. akcji, walut, surowców), pełni istotną rolę w zarządzaniu ryzykiem finansowym. Główne funkcje tego rynku to zabezpieczanie ryzyka (hedging), gdzie inwestorzy wykorzystują kontrakty terminowe do ochrony przed niekorzystnymi zmianami cen aktywów, spekulacja, polegająca na osiąganiu zysków na zmianach cen, oraz arbitraż, czyli wykorzystywanie różnic cenowych między rynkami w celu osiągnięcia bezpiecznych zysków[86]. Ostatnim segmentem jest rynek depozytowo-kredytowy, obejmujący działalność banków komercyjnych oraz innych instytucji finansowych, które oferują usługi związane z gromadzeniem oszczędności oraz udzielaniem kredytów. Jego podstawowe funkcje to mobilizacja oszczędności, gdzie gospodarstwa domowe i przedsiębiorstwa lokują nadwyżki finansowe na lokatach bankowych, finansowanie działalności gospodarczej poprzez udzielanie kredytów na rozwój przedsiębiorstw i konsumpcję indywidualną, oraz zarządzanie ryzykiem finansowym, w ramach którego banki stosują procedury oceny zdolności kredytowej i dywersyfikację portfela kredytowego[87]. Każdy z tych segmentów pełni istotną rolę w

---

[84] Yavorska, V. (2022). ANALYSIS OF CAPITAL MARKETS AND ORGANIZED COMMODITY MARKETS. *Market Infrastructure*. https://doi.org/10.32782/infrastruct69-5.

[85] Novak, O., Osadcha, T., & Petruk, O. (2019). CONCEPT AND CLASSIFICATION OF DERIVATIVE FINANCIAL INSTRUMENTS AS A METHODOLOGICAL PRECISION ON THEIR REGULATION IN THE FINANCIAL SERVICES MARKET. *Baltic Journal of Economic Studies*. https://doi.org/10.30525/2256-0742/2019-5-3-135-144.

[86] Miljkovic, L. (2023). THE ROLE OF FINANCIAL DERIVATIVES IN FINANCIAL RISKS MANAGEMENT. *MEST Journal*. https://doi.org/10.12709/mest.11.11.01.09.

[87] Carletti, E., Leonello, A., & Marquez, R. (2024). Market Power in Banking. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4691168.

stabilizacji i rozwoju gospodarki, a ich wzajemne powiązania i efektywne funkcjonowanie stanowią podstawę stabilności globalnego systemu finansowego.

Cyfryzacja oraz rozwój technologii mają ogromny wpływ na funkcjonowanie wszystkich segmentów rynków finansowych[88]. Platformy elektroniczne, automatyzacja procesów transakcyjnych oraz zaawansowane narzędzia analityczne zrewolucjonizowały sposób działania rynków, zwiększając ich dostępność oraz efektywność. Jednocześnie rosnąca zależność od technologii wiąże się z ryzykiem cyberzagrożeń, które mogą zakłócać funkcjonowanie systemów i prowadzić do poważnych strat finansowych. Rynek akcji, na przykład, narażony jest na manipulacje algorytmiczne, podczas gdy rynek instrumentów pochodnych zmaga się z wyzwaniami związanymi z dużą zmiennością i potencjalnymi błędami w systemach transakcyjnych[89].

Podsumowując, segmentacja rynków finansowych odzwierciedla ich różnorodność oraz złożoność, które są kluczowe dla efektywnego funkcjonowania współczesnej gospodarki. Każdy z segmentów pełni specyficzną rolę, zapewniając narzędzia do alokacji kapitału, zarządzania ryzykiem czy wspierania płynności finansowej. Jednocześnie postępująca globalizacja, cyfryzacja oraz zmieniające się otoczenie regulacyjne stawiają przed rynkami nowe wyzwania, wymagające dalszego rozwoju oraz adaptacji do dynamicznie zmieniających się warunków. W kolejnych częściach pracy szczegółowo omówione zostaną ryzyka i podatność poszczególnych segmentów na zagrożenia cyfrowe.

3. Instrumenty f nansowe a ich podatność na zagrożenia cyfrowe

Instrumenty finansowe stanowią podstawowy element funkcjonowania współczesnych rynków finansowych, pełniąc kluczową rolę w procesach alokacji kapitału oraz zarządzania ryzykiem. W literaturze przedmiotu są definiowane jako umowy zawierane pomiędzy uczestnikami rynku, określające ich wzajemne prawa i obowiązki w zakresie przepływów

[88] Blazhevich, O., & Safonova, N. (2022). FEATURES OF THE FINANCIAL MARKET DEVELOPMENT IN THE CONDITIONS OF DIGITALIZATION. *Scientific Bulletin: finance, banking, investment.*. https://doi.org/10.37279/2312-5330-2021-1-106-124.
[89] Blazhevich, O., & Safonova, N. S. (2022). Features of the Financial Market Development in the Conditions of Digitalization. *Scientific Bulletin: Finance, Banking, Investment*. DOI: 10.37279/2312-5330-2021-1-106-124

pieniężnych lub transferu aktywów[90]. W zależności od celu zastosowania, instrumenty te mogą służyć inwestowaniu, zabezpieczaniu się przed ryzykiem lub prowadzeniu działań spekulacyjnych. Klasyfikacja instrumentów finansowych obejmuje kilka głównych kategorii, z których każda charakteryzuje się odmiennymi właściwościami oraz zastosowaniem gospodarczym. Instrumenty pierwotne, zwane również tradycyjnymi lub bazowymi, posiadają niezależną wartość rynkową i są emitowane bezpośrednio przez podmioty gospodarcze. Do tej grupy zaliczają się instrumenty kapitałowe, takie jak akcje zwykłe, reprezentujące udział własnościowy w kapitale spółek, kwity depozytowe (ADR, GDR), które umożliwiają międzynarodowy obrót akcjami, czy udziały w spółkach kapitałowych[91]. Do instrumentów tradycyjnych należą również papiery dłużne, takie jak obligacje skarbowe emitowane przez rządy, obligacje korporacyjne i komunalne, certyfikaty depozytowe, weksle handlowe oraz listy zastawne emitowane przez banki hipoteczne. Kolejną istotną grupą są instrumenty pochodne (derywaty), których wartość uzależniona jest od cen aktywów bazowych – takich jak akcje, obligacje, waluty, surowce czy indeksy giełdowe. Instrumenty te pełnią kluczową rolę w zarządzaniu ryzykiem, spekulacji oraz arbitrażu. Należą do nich kontrakty terminowe (futures, forward), opcje, swapy oraz warranty[92]. Szczególnym rodzajem instrumentów są również instrumenty hybrydowe, łączące cechy instrumentów dłużnych i udziałowych, np. obligacje zamienne na akcje czy obligacje wieczyste, które nie posiadają określonego terminu zapadalności. Kolejna grupa to instrumenty strukturyzowane, takie jak obligacje strukturyzowane, których wypłata zależy od realizacji określonych scenariuszy rynkowych[93]. Ponadto, współczesny rynek finansowy charakteryzuje się dynamicznym rozwojem nowych technologii, które doprowadziły do powstania innowacyjnych instrumentów finansowych opartych na technologii blockchain, takich jak tokeny giełdowe (security tokens), smart contracts czy cyfrowe aktywa w formie kryptowalut[94]. Kolejnym istotnym rodzajem

---

[90] Kudła J., *Instrumenty finansowe i ich zastosowanie*, Key Text, Warszawa, 2022.s11

[91] Tamże, s. 27

[92] Garškaitė-Milvydienė, K. (2022). *Use of Derivative Financial Instruments for Risk Management.* DOI: 10.3846/bm.2022.793

[93] (2019). Hybrid finance instruments for SMEs (New Approaches to SME and Entrepreneurship Financing: Broadening the Range of Instruments). .

[94] Subramanian, H. (2019). Security tokens: architecture, smart contract applications and illustrations using SAFE. *Managerial Finance*. https://doi.org/10.1108/MF-09-2018-0467.

instrumentów są instrumenty ubezpieczeniowe i emerytalne, obejmujące produkty takie jak obligacje katastroficzne (CAT Bonds), fundusze emerytalne oraz instrumenty ubezpieczeniowe zabezpieczające przed specyficznymi rodzajami ryzyka[95]. Wszystkie wymienione rodzaje instrumentów finansowych pełnią zróżnicowane funkcje w gospodarce, od zapewnienia płynności i stabilności finansowej, poprzez pozyskiwanie kapitału na rozwój działalności gospodarczej, aż po zaawansowane metody zarządzania ryzykiem na poziomie operacyjnym oraz strategicznym. Ich kompleksowe wykorzystanie pozwala na efektywną alokację zasobów, redukcję ryzyka systemowego oraz wspieranie wzrostu gospodarczego. Należy zwrócić uwagę, że cyfryzacja rynków finansowych zrewolucjonizowała sposób, w jaki instrumenty finansowe są emitowane, obracane i przechowywane. Zastosowanie zaawansowanych technologii informatycznych, takich jak *blockchain*, sztuczna inteligencja czy algorytmiczne systemy transakcyjne, zwiększyło efektywność rynków i obniżyło koszty operacyjne. Jednak rosnąca zależność od technologii niesie za sobą nowe ryzyka i wyzwania, w tym także ryzyko cyberataków[96]. Jednym z najczęstszych zagrożeń dla instrumentów finansowych są ataki na platformy handlowe i systemy rozliczeniowe. Ataki typu DDoS, które polegają na przeciążeniu serwerów poprzez masowe wysyłanie prostych zapytań, mogą zakłócić funkcjonowanie giełd, prowadząc nawet do czasowego zawieszenia obrotu. W 2014 roku tego typu atak dotknął giełdę GPW w Warszawie, powodując czasowe zakłócenia w działaniu systemu transakcyjnego[97]. Jako kolejne poważne zagrożenie, możemy rozpatrywać ataki typu phishing, które mogą doprowadzić do wyłudzenia danych uwierzytelniających od uczestników rynku, co umożliwia cyberprzestępcom nieautoryzowany dostęp do kont inwestycyjnych. W przypadku akcji i obligacji, takie działania mogą prowadzić do nieuprawnionego zbycia instrumentów lub manipulacji cenami na rynku.

Instrumenty pochodne, które cechują się złożoną strukturą, są szczególnie podatne na zagrożenia cyfrowe wynikające z zaawansowanych manipulacji rynkowych. Algorytmiczne systemy tradingowe, które dominują w obrocie instrumentami pochodnymi, są narażone na

---

[95] Taylor, D. (2020). Modeling the Price Dynamics of Catastrophe Bonds. . https://doi.org/10.1184/R1/12830381.V1.

[96] Seo, J. (2018). Business Value of Blockchain and Applications of Artificial Intelligence. *Asia-Pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, 8*(7), 779–789. DOI: 10.35873/ajmahs.2018.8.7.076

[97] Byszewski, G., & Kozubal, M. (2014, październik 23). Nie działała strona giełdy. Atak hakerów? *Rzeczpospolita*. Dostępne na: https://www.rp.pl/kraj/art4833851-nie-dzialala-strona-gieldy-atak-hakerow (dostęp: 19.12.2024).

ataki polegające na wprowadzaniu fałszywych danych, tzw. *spoofingu*, gdzie przestępcy generują sztuczne zlecenia w celu wpłynięcia na ceny aktywów bazowych[98]. Przykładem zagrożenia specyficznego dla instrumentów pochodnych jest tzw. *flash crash*, czyli nagły, drastyczny spadek cen aktywów spowodowany błędami w algorytmach lub celowym działaniem cyberprzestępców. Tego typu incydenty miały miejsce na amerykańskim rynku *futures* w 2010 roku, kiedy algorytmiczne systemy transakcyjne zareagowały w sposób kaskadowy na gwałtowne zmiany w danych rynkowych, prowadząc do utraty miliardów dolarów w ciągu kilku minut[99].

Wraz ze wzrostem wyzwań i zagrożeń technologicznych rozwijają się także technologie zwiększające bezpieczeństwo. Jednym z najważniejszych osiągnięć w dziedzinie ochrony instrumentów finansowych przed zagrożeniami cyfrowymi jest technologia blockchain. Technologia ta dzięki zastosowaniu zdecentralizowanej struktury danych, umożliwia bezpieczne przechowywanie i wymianę informacji o transakcjach. W przypadku akcji i obligacji pozwala na np. transparentne rejestrowanie właścicieli oraz zmian w strukturze kapitałowej przedsiębiorstw, co w sposób zdecydowany zmniejsza ryzyko fałszerstw i nieuprawnionych transakcji[100]. Natomiast na rynku instrumentów pochodnych zdecentralizowane sieci *blockchain* mogą być wykorzystywane do automatyzacji procesów zawierania i rozliczania kontraktów dzięki zastosowaniu inteligentnych umów (smart contracts). Są one programowalnymi protokołami, które w sposób automatyczny wykonują zapisy kontraktowe, eliminując potrzebę interwencji stron trzecich, co zwiększa efektywność i bezpieczeństwo transakcji[101].

Jednak mimo postępów technologicznych w dziedzinie ochrony, instrumenty finansowe pozostają narażone na nowe rodzaje zagrożeń, które pojawiają się w miarę rozwoju

[98] Wang, X., Hoang, C., & Wellman, M. (2019). Learning-Based Trading Strategies in the Face of Market Manipulation. *Proceedings of the First ACM International Conference on AI in Finance*. DOI: 10.1145/3383455.3422568

[99] Kirilenko, A., Kyle, A. S., Samadi, M., & Tuzun, T. (2017). The Flash Crash: High-Frequency Trading in an Electronic Market. *Economics of Networks eJournal*. DOI: 10.2139/ssrn.1686004

[100] Priyadarshana, D., Rao, T. R., & Rao, M. S. (2024). AI and blockchain technology for secure and transparent financial transactions. *International Journal of Science and Research Archive*. DOI: 10.30574/ijsra.2024.13.1.1845

[101] Jaiwani, M., Gopalkrishnan, S., Kale, V., Chatterjee, A., Khatwani, R., Kasam, N., & Mitra, P. K. (2023). The Blockchain Revolution: Disrupting Derivative Markets with Smart Contracts. *2023 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD)*, 1-7. DOI: 10.1109/ICTMOD59086.2023.10438145

technologicznego. Nowe możliwości ochrony daje wprowadzenie sztucznej inteligencji i uczenia maszynowego do zarządzania ryzykiem oraz analizy danych rynkowych, ale jednocześnie wiąże się z ryzykiem związanym z manipulacją algorytmami oraz błędami w ich projektowaniu[102]. Jako istotne wyzwaniem należy wskazać również dostosowanie regulacji prawnych do szybko zmieniającego się otoczenia technologicznego. Dyrektywy takie jak MiFID II oraz rozporządzenie NIS2 wymagają od instytucji finansowych wprowadzenia zaawansowanych mechanizmów ochrony danych oraz regularnego raportowania incydentów bezpieczeństwa, co stanowi istotny krok w kierunku zwiększenia odporności sektora finansowego na cyberzagrożenia.

Podsumowując, instrumenty finansowe są kluczowym elementem współczesnych rynków, ale ich funkcjonowanie wiąże się z rosnącym ryzykiem wynikającym z cyfryzacji i rozwoju technologii. Skuteczne zarządzanie tym ryzykiem wymaga inwestycji w nowoczesne systemy bezpieczeństwa, rozwój regulacji oraz edukację uczestników rynku w zakresie cyberbezpieczeństwa. Tylko dzięki zintegrowanemu podejściu możliwe będzie zapewnienie stabilności i efektywności globalnego systemu finansowego w obliczu dynamicznie zmieniających się warunków technologicznych i gospodarczych.

4. Ryzyka i podatność segmentów rynkowych na cyberataki

Rynki finansowe, które stanowią kluczowy element globalnej gospodarki, są narażone na różnorodne zagrożenia wynikające z postępującego rozwoju cyfryzacji i integracji technologicznej. Każdy z segmentów rynków finansowych charakteryzuje się specyficznym profilem ryzyka związanego z cyberatakami. W niniejszym rozdziale omówione zostaną najważniejsze ryzyka, zagrożenia oraz podatność poszczególnych segmentów rynkowych na ataki cyfrowe, ze szczególnym uwzględnieniem ich skutków dla stabilności i funkcjonowania globalnego systemu finansowego.

Rynek akcji pełni kluczową rolę w gospodarce, umożliwiając przedsiębiorstwom pozyskiwanie kapitału na rozwój, ale także inwestorom indywidualnym i instytucjonalnym uczestniczenie w podziale zysków. Niemniej jednak jego funkcjonowanie pozwala rozpoznać

[102] Xu, H., Niu, K., Lu, T., & Li, S. (2024). Leveraging artificial intelligence for enhanced risk management in financial services: Current applications and future prospects. *Engineering Science & Technology Journal*. DOI: 10.51594/estj.v5i8.1363

szereg potencjalnych i realnych zagrożeń wynikających z rozwoju technologii informacyjnej i wciąż rosnącej liczby ataków cybernetycznych. Jednym z najważniejszych ryzyk dla tego segmentu jest ryzyko ataków hakerskich związane m.in. z manipulacją cenami akcji, która może być przeprowadzana za pomocą np. złośliwych algorytmów lub ataków na platformy transakcyjne. Aby tego dokonać cyberprzestępcy mogą np. wpływać na ceny akcji poprzez rozprzestrzenianie fałszywych informacji na platformach społecznościowych lub dedykowanych portalach giełdowych, co może prowadzić do sztucznego podnoszenia lub obniżania wartości wybranych instrumentów[103]. Wskazane manipulacje mogą powodować straty finansowe dla inwestorów, ale równieżwpływać na stabilność całego rynku. Przykładem takiego ataku była sytuacja z 2021 roku, kiedy manipulacje na akcjach GameStop doprowadziły do ekstremalnych wahań cen, co ukazało podatność rynków na działania skoordynowane przez uczestników społeczności internetowych[104]. Kolejnym ryzykiem jest wyciek danych związany z bezpośrednimi atakami na informatyczne systemy giełdowe, takie jak platformy transakcyjne, czy też systemy rozliczeniowe. W takim przypadku ataki typu DDoS mogą skutecznie uniemożliwić dostęp do platform handlowych, co z kolei może prowadzić do zakłóceń w realizacji zleceń i stwarzać ryzyko potencjalnych strat finansowych. Dodatkowo, np. nieautoryzowany dostęp do kont inwestorów może w konsekwencji skutkować przeprowadzeniem niepożądanych transakcji lub wyciekiem danych chronionych. Problemy te podkreślają jak bardzo istotna jest potrzeba ciągłego rozwoju zabezpieczeń technologicznych i świadomości uczestników rynku. Kolejnym bardzo ważnym elementem cyberzagrożeń dla rynku akcji są także potencjalne manipulacje algorytmicznych systemów tradingowych. W takim przypadku cyberprzestępcy mogą wykorzystać luki w algorytmach, wprowadzając fałszywe dane lub generując sztuczne zlecenia (tzw. *spoofing*), co destabilizuje ceny i powoduje zakłócenia na rynku. Obserwuje się jednak, że w miarę zwiększania się roli technologii w funkcjonowaniu rynku akcji, zagrożenia cybernetyczne stają się coraz bardziej wyrafinowane, co z kolei wymaga wdrażania zaawansowanych i kosztownych mechanizmów monitorowania i reagowania na incydenty[105].

[103] Mahajan, S., & Morya, S. (2024). Analysis of the Interplay of Hacking and Its Effects on Financial Market. *Nanotechnology Perceptions*. DOI: 10.62441/nano-ntp.v20is9.53

[104] Long, S. C., Lucey, B., Xie, Y., & Yarovaya, L. (2022). "I Just Like the Stock": The Role of Reddit Sentiment in the GameStop Share Rally. *Financial Review*. DOI: 10.1111/fire.12328

[105] Geisler, K. (2018). Hacking Wall Street: Reconceptualizing Insider Trading Law for Computer Hacking and Trading Schemes. *White Collar Crime eJournal*. DOI: 10.2139/ssrn.3221987

W porównaniu z rynkiem akcji, rynek obligacji charakteryzuje się mniejszą zmiennością i wyższym poziomem stabilności, co czyni go bardziej atrakcyjnym dla inwestorów poszukujących bezpiecznych instrumentów inwestycyjnych. Jednak rosnąca cyfryzacja tego segmentu niesie ze sobą nowe zagrożenia związane z cyberatakami, które mogą wpływać także na jego funkcjonowanie. Jednym z największych wyzwań dla tego rynku są ataki na systemy rozliczeniowe, takie jak np. SWIFT czy inne platformy, których przeznaczeniem jest obsługa transakcje międzynarodowe[106]. Jak pokazuje historia, przypadki zakłóceń w funkcjonowaniu tych systemów mogą prowadzić do opóźnień w realizacji płatności, co z kolei wpływa na zaburzenia płynności finansowych emitentów oraz inwestorów. Doskonałym przykładem jest rok 2016, w którym to został zaatakowany przez hakerów system SWIFT. Cyberprzestępcy wykradli 81 milionów dolarów z banku centralnego Bangladeszu. Mimo, iż incydent ten nie dotyczył bezpośrednio rynku obligacji, to bezsprzecznie pokazuje, jak międzynarodowe systemy rozliczeniowe są podatne na ataki[107]. Jako dodatkowe zagrożenie należy wskazać kradzieże danych związanych z obligacjami korporacyjnymi, w tym m.in. szczegółowych informacji o emitentach i warunkach emisji. Tego typu dane w rękach cyberprzestępców mogą być wykorzystane do przeprowadzania manipulacji rynkowych lub szantażu emitentów. Ponadto, w sytuacji ataku na obligację zielone, w których ważną rolą jest transparentność i zgodność z określonymi standardami środowiskowymi, cyberataki mogą zaszkodzić reputacji emitentów, podważając wiarygodność certyfikatów ekologicznych[108].

Rynek walutowy, czyli najbardziej płynny z segmentów, charakteryzuje się 24-godzinną dostępnością, dużą zmiennością kursów oraz ogromną skalą transakcji, które wynoszą ponad 6 bilionów dolarów dziennie[109]. I właśnie te cechy czynią rynek walutowy szczególnie podatnym na różnorodne zagrożenia cybernetyczne, gdyż mogą zakłócać jego funkcjonowanie i prowadzić tym samym do poważnych strat finansowych. Jednym z największych zagrożeń dla rynku walutowego są ataki typu DDoS, których celem jest istotne przeciążenie systemów transakcyjnych i platform handlowych. Mogą one skutkować czasowym zawieszeniem

[106] Gilderdale, S. (2017). SWIFT's customer security programme: Preventing, detecting and responding to the growing cyber threat. *Journal of Securities Operations & Custody*. DOI: 10.69554/eicr3197
[107] Scott, B. (2016). The SWIFT Hack: How $81 Million Vanished in a Flash. *Financial Crime Review*. DOI: 10.2139/ssrn.2834321
[108] Estiningrum, W., & Husodo, Z. (2024). Identifying Green Bonds Impact on Company Reputation and Risk. *International Research Journal of Business Studies*. DOI: 10.21632/irjbs.17.1.1-19
[109] Bjønnes, G. H., Rime, D., & Solheim, H. O. (2019). The impact of different players on the volume-volatility relation in the foreign exchange market. *Beta*. DOI: 10.18261/ISSN.1504-3134-2019-01-04

działalności platform, które prowadzi do uniemożliwia inwestorom realizacji zleceń i w konsekwencji grozi destabilizacją rynku. Dodatkowo, cyberprzestępcy mogą także przeprowadzać manipulacje kursami walut poprzez fałszywe zlecenia, które z kolei w konsekwencji mogą wpływać na decyzje innych uczestników rynku i sztucznie generować zmienność kursów. Innym wyzwaniem dla rynku walutowego są natomiast tzw. boty handlowe. Ich celem, w rękach cyberprzestępców, jest zautomatyzowane wprowadzanie ogromnej liczby zleceń w krótkim czasie, co powoduje destabilizację rynku i znaczące wahania kursów walutowych[110]. Jako przykład można podać tzw. *flash crash* z 2016 roku, kiedy kurs funta brytyjskiego gwałtownie spadł w ciągu kilku minut, co było związane z działaniem algorytmów handlowych w odpowiedzi na fałszywe dane rynkowe[111]. Warto także zwrócić uwagę na ryzyko związane z rosnącą rolą kryptowalut na rynku walutowym. Cyfrowe aktywa, takie jak np. Bitcoin czy Ethereum, mimo że oferują nowe możliwości inwestycyjne, są również celem licznych ataków hakerskich na giełdy kryptowalutowe oraz na tzw. portfele cyfrowe. Liczne kradzieże kryptowalut, takie jak chociażby głośny przypadek Mt. Gox, gdzie z giełdy zniknęło ponad 850 tysięcy Bitcoinów[112], w sposób oczywisty pokazują, jak istotne jest wdrażanie skutecznych mechanizmów zabezpieczających w tym segmencie rynku walutowego.

Struktura rynku instrumentów pochodnych oraz rosnące wykorzystanie technologii czynią go szczególnie podatnym na cyberzagrożenia, które mogą prowadzić do poważnych zakłóceń w funkcjonowaniu całego systemu finansowego. Jednym z głównych zagrożeń dla tego rynku jest tzw. manipulacja algorytmiczna, która polega na wprowadzaniu fałszywych zleceń w celu sztucznego wpływania na ceny aktywów bazowych. Przykładem tego typu operacji jest praktyka *spoofingu*, gdzie cyberprzestępcy generują zlecenia kupna lub sprzedaży, które w dalszym kroku są anulowane, co z kolei ma wpłynąć na zachowania innych uczestników rynku. Tego typu działania, zgodnie ze swoimi zamierzeniami, mogą destabilizować rynek, prowadząc do gwałtownych zmian cen oraz strat finansowych dla inwestorów[113]. Jako dodatkowe ryzyko

[110] Vo, H. T. K., Wojciechowski, R., & Weinhardt, C. (2005). Integration of Electronic Foreign Exchange Trading and Corporate Treasury Systems with Web Services. *Lecture Notes in Computer Science, 3795*, 471–488. DOI: 10.1007/3-7908-1624-8_25

[111] Schroeder, F., Lepone, A., Leung, H., & Satchell, S. (2020). Flash crash in an OTC market: trading behaviour of agents in times of market stress. *The European Journal of Finance, 26*(12), 1569–1589. DOI: 10.1080/1351847x.2020.1748893

[112] McCorry, P., Möser, M., & Ali, S. (2018). Why Preventing a Cryptocurrency Exchange Heist Isn't Good Enough. W *Proceedings of the International Conference on Financial Cryptography and Data Security*, 225–233. DOI: 10.1007/978-3-030-03251-7_27

[113] Cartea, Á., Jaimungal, S., & Wang, Y. (2020). Spoofing and Price Manipulation in Order-Driven Markets. *Applied Mathematical Finance, 27*(1), 67–98. DOI: 10.1080/1350486X.2020.1726783

należy wymienić ataki na systemy obliczeniowe obsługujące rozliczenia kontraktów pochodnych. Z uwagi na wspomnianą wcześniej dużą złożoność tych instrumentów, systemy te wymagają zaawansowanych algorytmów do kalkulacji wartości rynkowej oraz rozliczeń finansowych. Dlatego nieautoryzowany dostęp do tego typu systemów może umożliwić cyberprzestępcom manipulację danymi, co w rezultacie prowadzi do nieprawidłowego rozliczenia kontraktów i tym samym strat dla zaangażowanych stron. Jednym z prawdopodobnie najbardziej spektakularnych przykładów zagrożeń na rynku instrumentów pochodnych był błąd algorytmu tradingowego firmy Knight Capital w 2012 roku, który doprowadził do strat sięgających 440 milionów dolarów w ciągu zaledwie jednego dnia[114].

Ryzyko związane z cyberatakami stało się jednym z najpoważniejszych wyzwań dla współczesnych rynków finansowych. Dlatego należy zwrócić uwagę, że każdy z segmentów rynku — charakteryzuje się unikalną podatnością na zagrożenia wynikające z dynamicznego rozwoju technologii i globalizacji. Jednak wspólnym elementem wszystkich zagrożeń jest rosnąca zależność rynków od technologii cyfrowych oraz algorytmicznych systemów tradingowych. Cyberprzestępcy korzystający z coraz bardziej wyrafinowanych metod, częściej wykorzystują luki w zabezpieczeniach, aby manipulować rynkami lub zakłócać ich funkcjonowanie, co prowadzi do strat finansowych, ale także podważa stabilność całego systemu finansowego. Dlatego też odpowiedzią na te wyzwania powinno być rozwijanie zaawansowanych technologii bezpieczeństwa oraz wdrażanie mechanizmów monitorowania i szybkiego reagowania na incydenty. Współpraca między instytucjami finansowymi, regulatorami oraz dostawcami technologii jest nieodzowna dla ograniczenia podatności rynków finansowych na cyberzagrożenia. Zapewnienie bezpieczeństwa w każdym segmencie rynku ma kluczowe znaczenie dla zachowania ich stabilności i zaufania uczestników, co przekłada się na efektywność globalnego systemu finansowego.

[114] Pereira, C. M. (2020). Unregulated Algorithmic Trading: Testing the Boundaries of the European Union Algorithmic Trading Regime. *Journal of Financial Regulation, 6*(3), 270–305. DOI: 10.1093/jfr/fjaa008

5. Sektor bankowy, instytucje płatnicze, giełdy w kontekście cyfryzacji

Cyfryzacja wpłynęła na kluczowe aspekty funkcjonowania sektora bankowego, instytucji płatniczych i giełd, zmieniając zarówno sposób świadczenia usług, jak i ich znaczenie w globalnym systemie finansowym. Rozwój technologii cyfrowych był jednym z głównych czynników, dzięki któremu instytucje te stały się bardziej dostępne i efektywne, choć jednocześnie napotykają nowe wyzwania związane z ich bezpieczeństwem i podatnością na incydenty cybernetyczne.

Sektor bankowy od zawsze odgrywał kluczową rolę w gospodarce, ale cyfryzacja pozwoliła na jeszcze szerszy zakres usług i realną zaawansowaną integrację z codziennym życiem klientów. W toku rewolucji cyfrowej tradycyjne banki stacjonarne uzupełniły swoją działalność o bankowość internetową i mobilną, co znacznie zwiększyło dostępność usług. Dzięki tego typu rozwiązaniom klienci mogą zarządzać swoimi finansami z dowolnego miejsca na świecie, co kompletnie zrewolucjonizowało sposób korzystania z produktów finansowych[115]. Ponadto, cyfryzacja umożliwiła również rozwój systemów natychmiastowych przelewów i elektronicznych systemów rozliczeń międzybankowych, do których można zaliczy systemy typu SEPA czy krajowe systemy do obsługi płatności w czasie rzeczywistym. Dzięki tego typu rozwiązaniom udało się osiągnąć przyspieszenie procesów finansowych i obniżenie kosztów transakcyjnych, co jest szczególnie istotne w dynamicznie zmieniającym się środowisku globalnym[116]. Jednak wraz z cyfrowym przekształceniem sektora bankowego pojawiły się również nowe wyzwania. Banki muszą sprostać oczekiwaniom klientów dotyczącym szybkości i wygody, przy czym jednocześnie zapewniając najwyższy poziom bezpieczeństwa. Co istotne w kontekście cyberbezpieczeństwa - technologia umożliwiła nie tylko przyspieszenie

[115] Nalini, R., & Yuvasri, S. (2024). A Study on the Impact of Digital Transformation in the Banking Sector on Customer's Experience. *International Journal of Innovative Research in Engineering and Management*. DOI: 10.55524/ijirem.2024.11.2.8

[116] Natarajan, H., & Balakrishnan, M. (2020). Real-time retail payments system or faster payments: Implementation considerations. *Journal of Payments Strategy & Systems*. DOI: 10.69554/oejb5155

procesów, ale również zwiększyła ich złożoność, co wymaga inwestycji w nowoczesną infrastrukturę oraz ciągłe doskonalenie systemów zarządzania ryzykiem[117].

Instytucje płatnicze, takie jak np. operatorzy kart płatniczych, platformy cyfrowe oraz fintechy, odgrywają coraz większą rolę w cyfrowej gospodarce. Dzięki rozwojowi technologii umożliwiono realizację płatności w czasie rzeczywistym, bez względu na lokalizację geograficzną stron transakcji. Popularność płatności mobilnych oraz aplikacji takich jak Google Pay, Apple Pay czy Revolut przyczyniła się do wzrostu liczby bezgotówkowych transakcji na całym świecie. Na uwagę zwraca fakt, że cyfryzacja instytucji płatniczych była szczególnie widoczna w czasie pandemii COVID-19, kiedy nastąpił gwałtowny wzrost zainteresowania płatnościami bezkontaktowymi oraz zakupami online. Dzięki nowym technologiom, jakimi są np. Near Field Communication (NFC) czy też szybkie przelewy P2P, ich użytkownicy mogli realizować transakcje w sposób szybki, wygodny i bezpieczny[118]. Kolejnym aspektem w kontekście cyfryzacji jest wzrost znaczenie instytucji płatniczych w promowaniu inkluzji finansowej. To właśnie dzięki dostępowi do rozwiązań mobilnych osoby, które wcześniej nie miały lub miały utrudniony dostęp do tradycyjnych usług bankowych, mogą teraz uczestniczyć w życiu gospodarczym. Jako przykład można wymienić system M-Pesa w Afryce, który umożliwia realizację płatności oraz transferów pieniędzy za pomocą telefonów komórkowych, bez potrzeby posiadania nawet konta bankowego[119].

Giełdy finansowe, jako centralne platformy obrotu instrumentami finansowymi, również zostały głęboko zmienione przez cyfryzację. To właśnie rozwój technologii informatycznych sprawiły, że tradycyjne parkiety handlowe, takie jak NYSE czy GPW w Warszawie, przekształciły się w elektroniczne systemy obrotu, które umożliwiają realizację tysięcy transakcji w ułamku sekundy. Spowodowało to zwiększenie efektywności, płynność oraz dostępność giełd dla inwestorów nie zależnie od lokalizacji geograficznej. Dodatkowo cyfrowe platformy transakcyjne przyczyniły się do popularyzacji inwestowania wśród klientów

[117] Kawimbe, S., & Kwalombota, M. (2024). Mitigating Cybersecurity Risks in the Digitization of Banking Operations: Strategies, Challenges, and Best Practices for Zambian Commercial Banks. *International Journal of Research and Innovation in Social Science*. DOI: 10.47772/ijriss.2024.803213s

[118] Macierzyński, W., & Macierzyński, M. (2023). Development of new payment services and the role of the fintech sector during the COVID-19 pandemic. *Central European Review of Economics & Finance*. DOI: 10.24136/ceref.2023.014

[119] Ndung'u, N. (2018). The M-Pesa Technological Revolution for Financial Services in Kenya: A Platform for Financial Inclusion. W *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2*, 37–56. DOI: 10.1016/B978-0-12-810441-5.00003-8

detalicznych, dzięki oferowaniu niskich kosztów transakcji oraz wprowadzając intuicyjne interfejsy użytkownika. Na uwagę zasługuje też fakt, że giełdy stały się bardziej zintegrowane z globalnym systemem finansowym, co zwiększa ich znaczenie dla stabilności rynków kapitałowych[120].

Sektor bankowy, instytucje płatnicze i giełdy zwiększają swój stopień integracji dzięki technologii cyfrowej. Dla przykładu banki korzystają z usług instytucji płatniczych, aby oferować klientom szybkie przelewy i płatności, podczas gdy giełdy umożliwiają bankom i inwestorom obrót instrumentami finansowymi. To właśnie cyfryzacja umożliwiła efektywne zarządzanie tymi procesami, co pozwoliło z kolei na większą dostępność kapitału i usprawniło przepływ środków w gospodarce. Jednak jednocześnie rosnąca integracja niesie ze sobą również bardzo duże wyzwania związane w szczególności z zależnością od infrastruktury technologicznej. Dlatego awaria w jednym z elementów systemu, np. na dużej giełdzie lub w systemie płatniczym, może prowadzić do zakłóceń w całym ekosystemie finansowym. Dlatego inwestycje w stabilność i niezawodność technologii są niezbędne dla zachowania funkcji tych instytucji w globalnym środowisku cyfrowym.

Podsumowując, cyfryzacja zmieniła sposób funkcjonowania sektora bankowego, instytucji płatniczych i giełd, zwiększając ich znaczenie oraz dostępność. Jednocześnie instytucje te muszą odpowiadać na wyzwania związane z dynamicznie rozwijającym się środowiskiem technologicznym, aby sprostać oczekiwaniom klientów oraz zapewnić stabilność globalnego systemu finansowego.

6. Znaczenie handlu algorytmicznego z zastosowaniem sztucznej inteligencji na rynkach f nansowych oraz potencjalne zagrożenia wynikające z automatyzacji handlu

Handel algorytmiczny (ang. *algo-trading*) wraz ze wsparciem wykorzystania sztucznej inteligencji (AI) na rynkach finansowych odgrywają kluczową rolę w kształtowaniu

[120] Rani, P., & Srinivasan, A. (2015). Digitization of Financial Markets: Impact and Future. *International Journal of Research in Finance and Marketing, 5*(29–33).

współczesnych mechanizmów obrotu. Technika ta bazuje na automatycznych algorytmach, które podejmują decyzje inwestycyjne w ułamkach sekundy i jest obecnie dominującą formą handlu na wielu rynkach, szczególnie w krajach rozwiniętych zmian rynkowych[121]. Pod względem technologicznym Algo-trading wykorzystuje algorytmy matematyczne i logiczne, które są zaprogramowane w taki sposób, aby reagowały na dane rynkowe w czasie rzeczywistym. Główne cele tych algorytmów skupiają się na optymalizacji procesów inwestycyjnych, redukcji kosztów transakcyjnych oraz minimalizacji ryzyka. Umożliwiają one:

- Natychmiastowe wykonywanie transakcji w odpowiedzi na zmiany cen.
- Arbitraż – wykorzystanie różnic cenowych między rynkami w celu generowania zysków.
- Reagowanie na zmienność – dostosowywanie strategii handlowych w zależności od warunków rynkowych[122].

Wykorzystanie AI wnosi do *algo-tradingu* dodatkową zdolność analizy danych na niespotykaną dotąd skalę. Dzieje się tak, gdyż w odróżnieniu od tradycyjnych algorytmów, które działają według ustalonych reguł, AI potrafi uczyć się na podstawie historycznych danych i dostosowywać swoje decyzje w sposób dynamiczny. Dzięki temu *algo-trading* zyskuje:

- Zwiększoną precyzję decyzji – AI potrafi analizować ogromne liczby danych rynkowych, prognozować trendy oraz dostosowywać strategie w odpowiedzi na zmieniające się warunki.
- Szybkość działania – AI integruje dane rynkowe zewnętrzne i wewnętrzne w czasie rzeczywistym, co pozwala na niemal natychmiastowe podejmowanie decyzji handlowych.
    - Zdolność do przewidywania zjawisk rynkowych – AI analizuje dane z szerokiego zakresu źródeł, takich jak media finansowe czy sygnały makroekonomiczne

[121] Addy, W. A., Ajayi-Nifise, A. O., Bello, B. G., Tula, S. T., Odeyemi, O., & Falaiye, T. (2024). Algorithmic Trading and AI: A Review of Strategies and Market Impact. *World Journal of Advanced Engineering Technology and Sciences*. DOI: 10.30574/wjaets.2024.11.1.0054

[122] Bacidore, J. M., Wu, D., & Xu, W. (2013). Balancing Execution Risk and Trading Cost in Portfolio Trading Algorithms. *The Journal of Trading, 8*(4), 37–43. DOI: 10.3905/jot.2013.8.4.037

Handel algorytmiczny znacząco zmienił sposób funkcjonowania rynków finansowych, przynosząc zarówno korzyści, jak i nowe wyzwania. Do pozytywnych aspektów *algo-tradingu* należą:

- Zwiększenie efektywności rynków – dzięki natychmiastowej realizacji transakcji i szybkiej reakcji na zmiany, *algo-trading* redukuje asymetrię informacyjną i zwiększa płynność rynków.
- Obniżenie kosztów transakcyjnych – automatyzacja obrotu pozwala na redukcję opłat związanych z handlem, co jest korzystne zarówno dla instytucji finansowych, jak i inwestorów detalicznych.
- Wzrost konkurencyjności – *algo-trading* zwiększa presję na uczestników rynku, zmuszając ich do doskonalenia strategii i efektywniejszego zarządzania portfelami.

Handel algorytmiczny mimo oczywistych korzyści, wiąże się także z poważnymi wyzwaniami i zagrożeniami, które mogą wpływać destabilizująco na rynki finansowe. Jednym z najbardziej znanych incydentów związanych z tą technologią był Flash Crash w 2010 roku, gdy indeks Dow Jones Industrial Average spadł o 9% w ciągu kilku minut, po czym niemal natychmiast wrócił do poprzednich poziomów. Jak stwierdziły późniejsze dochodzenia, zdarzenie to było wynikiem tzw. kaskadowych reakcji algorytmów na nietypowe zmiany rynkowe, co oznaczało, że wiele z nich równocześnie wprowadziło zlecenia sprzedaży, podążając za gwałtownym trendem spadkowym. Tego typu kaskadowe reakcje mogą prowadzić do gwałtownych wahań cen aktywów, które nie znajdują rynkowych uzasadnień[123]. Problem ten nasila się w sytuacjach wysokiej bardzo zmienności, kiedy algorytmy wzajemnie reagują na swoje działania, pogłębiając istniejące trendy. Z kolei innym poważnym wyzwaniem są manipulacje rynkowe, które mogą być realizowane przy użyciu konkretnych strategii algorytmicznych, do takich można zaliczyć spoofing czy layering. Spoofing polega na składaniu dużych zleceń kupna lub sprzedaży, które są następnie anulowane przed realizacją, co pozwala na sztuczne podnoszenie lub obniżanie cen aktywów i wpływanie na decyzje innych uczestników rynku. Z kolei layering to praktyka polegająca na składaniu licznych niewielkich zleceń na różnych poziomach cenowych w celu wywołania iluzji zainteresowania danym

[123] Easley, D., López de Prado, M. M., & O'Hara, M. (2011). The Microstructure of the "Flash Crash": Flow Toxicity, Liquidity Crashes, and the Probability of Informed Trading. *The Journal of Portfolio Management, 37*(2), 118–128. DOI: 10.3905/jpm.2011.37.2.118

aktywem. Obie strategie są trudne do wykrycia, ponieważ działania algorytmów odbywają się w milisekundach, co utrudnia organom nadzorczym reagowanie w odpowiednim czasie[124].

Należy też zwrócić uwagę na fakt, że *algo-trading* opiera się na zaawansowanej infrastrukturze technologicznej, co z kolei czyni go podatnym na różnorodne problemy techniczne i cyberataki. Awarie systemów, mogą prowadzić do zakłóceń w handlu, a nawet poważnych strat finansowych i destabilizacji całego rynku. Dodatkowym zagrożeniem są różnego rodzaju cyberataki. Zależność *algo-tradingu* od technologii oznacza, że awarie jednego elementu infrastruktury mogą mieć kaskadowe skutki, prowadząc do zakłóceń w funkcjonowaniu całego systemu finansowego. Natomiast wzajemne powiązania między algorytmami oraz ich integracja z różnymi rynkami finansowymi zwiększają ryzyko systemowe. Dzieje się tak, gdyż awaria lub nieprawidłowe działanie algorytmu na jednym rynku może wywołać zakłócenia na innych rynkach, a zwłaszcza gdy algorytmy korzystają z tych samych źródeł danych lub podejmują decyzje w oparciu o podobne założenia. Ponadto w sytuacjach kryzysowych, takich jak nagłe załamanie cen na rynku akcji lub obligacji, algorytmy mogą dodatkowo pogłębiać problem[125]. Dlatego te zagrożenia podkreślają konieczność wprowadzenia skutecznych regulacji, lepszych zabezpieczeń technologicznych oraz transparentności w działaniu algorytmów. Można tego dokonać poprzez wprowadzenie odpowiednich mechanizmów kontrolnych, takich jak testy warunków skrajnych czy też raportowanie strategii handlowych. Wydaje się to być kluczowe dla ograniczenia ryzyka destabilizacji rynku i utrzymania zaufania uczestników rynku. Przykładem takich regulacji jest dyrektywa MiFID II[126] wprowadzona w Unii Europejskiej, która nakłada na instytucje korzystające z *algo-tradingu* obowiązek raportowania oraz testowania algorytmów w celu minimalizacji ryzyka destabilizacji rynku[127].

[124] Leonard, G., Cao, Y., Haas, M., & Mocek, G. (2020). The legal and economic implications from recent UK spoofing cases. *Journal of Financial Compliance*. DOI: 10.69554/mlhq9467

[125] Min, B. H., & Borch, C. (2021). Systemic failures and organizational risk management in algorithmic trading: Normal accidents and high reliability in financial markets. *Social Studies of Science, 52*(2), 277–302. DOI: 10.1177/03063127211048515

[126] Parlament Europejski i Rada Unii Europejskiej, *Dyrektywa 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych (MiFID II)*, Dz.U. UE L 173 z 12.6.2014, s. 349–496.

[127] Busch, D. (2016). MiFID II: Regulating High Frequency Trading, Other Forms of Algorithmic Trading and Direct Electronic Market Access. *Law and Financial Markets Review, 10*(1), 72–82. DOI: 10.1080/17521440.2016.1200333

W miarę postępu technologicznego *algo-trading* będzie odgrywał coraz większą rolę na rynkach finansowych. Wdrożenie zaawansowanych technologii, takich jak *blockchain* czy przetwarzanie danych w chmurze, umożliwi jeszcze szybszy i bardziej efektywny handel. Jednocześnie konieczne będzie dalsze doskonalenie mechanizmów monitorowania i regulacji, aby zapewnić stabilność i bezpieczeństwo rynków. Podsumowując, handel algorytmiczny i sztuczna inteligencja zrewolucjonizowały rynki finansowe, wprowadzając nowe możliwości i wyzwania. Ich rozwój wymaga jednak odpowiedzialnego podejścia, które uwzględni zarówno korzyści, jak i ryzyka związane z technologią. Rynki finansowe przyszłości będą w coraz większym stopniu zależne od automatyzacji, co czyni algo-trading jednym z najważniejszych elementów współczesnego systemu finansowego.

7. Wyzwania związane z wykorzystaniem AI w f nansach

Sztuczna inteligencja (AI) odgrywa coraz większą rolę w sektorze finansowym, przynosząc znaczące korzyści w obszarach takich jak chociażby zarządzanie ryzykiem, analiza danych czy personalizacja usług. Jednak wraz ze wzrostem jej znaczenia pojawiają się wiele istotne wyzwania, które wymagają odpowiedniego zrozumienia, zarządzania oraz regulacji. Obejmują one nie tylko kwestie technologiczne, ale i etyczne oraz regulacyjne, które mogą wpływać na stabilność rynku, zaufanie uczestników i efektywność zastosowań AI.

Jednym z głównych wyzwań związanych z wykorzystaniem AI w finansach jest *złożoność technologiczna* systemów opartych na uczeniu maszynowym. Modele AI, szczególnie te oparte na *deep learningu*, są niezwykle skomplikowane i działają na podstawie ogromnych zbiorów danych. Choć pozwala to na precyzyjną analizę i przewidywanie zjawisk finansowych, jednocześnie zwiększa ryzyko wystąpienia błędów wynikających z nieprzewidzianych zależności w danych. Błędy w działaniu modeli AI mogą prowadzić do poważnych konsekwencji. Na przykład algorytmy podejmujące decyzje inwestycyjne mogą generować straty finansowe, jeśli interpretacja danych będzie nieprawidłowa[128]. Innym wyzwaniem jest problem tzw. „czarnej skrzynki" AI. Modele uczące się często działają w sposób nieprzejrzysty,

[128] Daiya, H. (2024). AI-Driven Risk Management Strategies in Financial Technology. *Journal of Artificial Intelligence General Science (JAIGS)*. DOI: 10.60087/jaigs.v5i1.194

co utrudnia wyjaśnienie, dlaczego podjęły określoną decyzję. W sektorze finansowym, gdzie zaufanie i transparentność są kluczowe, brak możliwości pełnego zrozumienia mechanizmu działania algorytmów może budzić nieufność klientów i regulatorów. Problem ten jest szczególnie istotny w przypadku decyzji dotyczących kredytów czy ubezpieczeń, gdzie AI ocenia zdolność kredytową lub ryzyko klienta na podstawie danych, których analiza może być subiektywnie interpretowana jako dyskryminacyjna. Kwestia biasu (tj. systematycznych odchyleń w danych prowadzących do faworyzowania lub dyskryminowania określonych grup lub wyników) to kolejne poważne wyzwanie[129]. Modele AI są zależne od jakości danych, na których są trenowane. Jeśli dane te zawierają historyczne błędy, nierówności lub schematy uprzywilejowania określonych grup, algorytm może je odtworzyć lub nawet wzmocnić. W kontekście finansów oznacza to ryzyko niesprawiedliwego traktowania klientów, na przykład poprzez odrzucanie wniosków kredytowych określonych grup społecznych lub geograficznych[130]. Utrzymanie jakości danych oraz opracowanie metod wykrywania i eliminacji uprzedzeń jest zatem kluczowe dla sprawiedliwego wykorzystania AI.

Cyberbezpieczeństwo stanowi kolejne wyzwanie związane z implementacją AI w finansach. Algorytmy AI, szczególnie te wykorzystywane w analizie rynkowej i tradingu, są atrakcyjnym celem dla cyberprzestępców. W przypadku przejęcia algorytmu przez nieuprawnione osoby może dojść do manipulacji rynkowej, kradzieży danych lub zakłócenia funkcjonowania całego systemu finansowego. Jednocześnie modele AI mogą być podatne na ataki polegające na wprowadzaniu fałszywych danych (tzw. adversarial attacks), które celowo wprowadzają algorytm w błąd, co prowadzi do niewłaściwych decyzji[131]. Kolejnym istotnym wyzwaniem są *kwestie regulacyjne*. Wykorzystanie AI w finansach jest nowym obszarem, który wymaga dostosowania istniejących ram prawnych do specyfiki technologii. Regulacje muszą uwzględniać potrzebę równowagi między innowacyjnością a ochroną klientów i stabilnością rynków. Niezbędne są mechanizmy umożliwiające audyt algorytmów, ich transparentność oraz weryfikację zgodności z zasadami etycznymi. Brak odpowiednich regulacji może prowadzić

---

[129] Fazil, A., Hakimi, M., & Shahidzay, A. (2024). A COMPREHENSIVE REVIEW OF BIAS IN AI ALGORITHMS. *Nusantara Hasana Journal*. https://doi.org/10.59003/nhj.v3i8.1052.

[130] Chopra, P. (2024). Ethical Implications of AI in Financial Services: Bias, Transparency, and Accountability. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. DOI: 10.32628/cseit241051017

[131] Peter, I., Ijiga, M., Olajide, F. I., & Olatunde, T. I. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention *Open Access Research Journal of Science and Technology*. DOI: 10.53022/oarjst.2024.11.1.0060

do chaosu na rynku, podczas gdy nadmierna liczba regulacji prawnych mogłaby zahamować rozwój innowacyjnych technologii[132].

Wyzwaniem jest również *rozwijanie kompetencji* w zakresie AI wśród pracowników sektora finansowego. Wprowadzenie zaawansowanych systemów wymaga wiedzy i umiejętności w ich obsłudze, monitorowaniu i rozwoju. Brak odpowiednio wykwalifikowanej kadry może prowadzić do niewłaściwego wykorzystania potencjału AI lub problemów w przypadku awarii systemów. Z kolei odpowiednie szkolenia i inwestycje w rozwój kompetencji mogą znacząco zwiększyć efektywność wdrażania sztucznej inteligencji.

Wreszcie, jednym z kluczowych wyzwań jest *zachowanie równowagi między automatyzacją a rolą człowieka*. Choć AI pozwala na automatyzację wielu procesów, decyzje o dużym znaczeniu, takie jak inwestycje na wielką skalę czy ocena ryzyka systemowego, nadal powinny być podejmowane przez ludzi, którzy mogą uwzględnić kontekst i czynniki niemierzalne.

Ostatecznie, przyszłość AI w finansach zależy od umiejętnego zarządzania jej potencjałem i ryzykiem. Dlatego wyzwania związane z implementacją sztucznej inteligencji wymagają kompleksowego podejścia, które obejmuje zarówno aspekty technologiczne, jak i społeczne oraz regulacyjne. Tylko dzięki odpowiedniemu zarządzaniu tymi kwestiami można w pełni wykorzystać korzyści płynące z AI, jednocześnie minimalizując ryzyka i zapewniając stabilność oraz zaufanie na rynkach finansowych[133]. Wraz z rosnącym zastosowaniem AI w finansach pojawia się również kwestia wpływu tej technologii na konkurencyjność sektora oraz jego strukturalne zmiany. Firmy, które z powodzeniem wdrażają AI, zyskują znaczącą przewagę nad podmiotami, które opierają się na tradycyjnych modelach biznesowych. Algorytmy pozwalają na szybsze i bardziej precyzyjne podejmowanie decyzji, co zwiększa efektywność operacyjną oraz zdolność do generowania zysków. Zjawisko to prowadzi jednak do koncentracji rynku, gdzie tylko największe instytucje finansowe z odpowiednimi zasobami technologicznymi są w stanie konkurować na najwyższym poziomie. W rezultacie mniejsze

[132] Deshpande, A. S. (2024). Regulatory Compliance and AI: Navigating the Legal and Regulatory Challenges of AI in Finance. *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*, 1, 1–5. DOI: 10.1109/ICKECS61492.2024.10616752

[133] **Yi Han, Jinhao Chen, Meitao Dou, Jiahong Wang, Kangxiao Feng** (2023). The Impact of Artificial Intelligence on the Financial Services Industry. *Academic Journal of Management and Social Sciences*. DOI: 10.54097/ajmss.v2i3.8741

podmioty mogą być zmuszone do konsolidacji lub rezygnacji z niektórych obszarów działalności, co ogranicza różnorodność sektora i zmniejsza konkurencję. Jednocześnie AI wpływa na zmiany w strukturze zatrudnienia w sektorze finansowym. Automatyzacja procesów dzięki AI prowadzi do zmniejszenia zapotrzebowania na pracowników w tradycyjnych obszarach, takich jak operacje bankowe czy obsługa klienta. W zamian za to rośnie zapotrzebowanie na specjalistów z zakresu analizy danych, programowania oraz zarządzania technologią. Zjawisko to stawia wyzwanie przed rynkiem pracy, który musi dostosować się do nowych wymagań, oraz przed instytucjami edukacyjnymi, które muszą oferować odpowiednie programy kształcenia w zakresie technologii AI[134]. Wdrażanie sztucznej inteligencji zmienia również relacje między instytucjami finansowymi a klientami. Dzięki analizie danych AI pozwala na personalizację usług, co prowadzi do bardziej precyzyjnego dopasowania ofert do potrzeb klientów. Jednocześnie jednak zwiększa to ryzyko naruszenia prywatności, gdyż algorytmy gromadzą i analizują ogromne liczby danych osobowych. Klienci mogą obawiać się, że ich dane są wykorzystywane w sposób, który nie jest dla nich transparentny, co podważa zaufanie do instytucji finansowych. W odpowiedzi na te obawy konieczne jest zapewnienie przejrzystości w sposobie wykorzystywania danych oraz wdrażanie odpowiednich mechanizmów ochrony prywatności. Dzięki analizie danych AI pozwala na personalizację usług, co prowadzi do bardziej precyzyjnego dopasowania ofert do potrzeb klientów. Jednocześnie jednak zwiększa to ryzyko naruszenia prywatności, gdyż algorytmy gromadzą i analizują ogromne ilości danych osobowych. Klienci mogą obawiać się, że ich dane są wykorzystywane w sposób, który nie jest dla nich transparentny, co podważa zaufanie do instytucji finansowych. W odpowiedzi na te obawy konieczne jest zapewnienie przejrzystości w sposobie wykorzystywania danych oraz wdrażanie odpowiednich mechanizmów ochrony prywatności.

Kolejnym wyzwaniem wynikającym z zastosowania AI jest *wpływ na stabilność systemu finansowego*. Modele AI, choć niezwykle zaawansowane, nie są wolne od ryzyka błędów lub niewłaściwej interpretacji danych, zwłaszcza w sytuacjach nietypowych lub kryzysowych. Ich nieprzewidywalność może prowadzić do sytuacji, w których wiele instytucji finansowych korzystających z podobnych modeli podejmuje jednocześnie podobne decyzje, co może nasilać

[134] Havryk, A., & Nazarova, T. (2024). Artificial intelligence and its role in the labor market and financial sector itself: US point of view. *International Science Journal of Management, Economics & Finance*. DOI: 10.46299/j.isjmef.20240303.01

efekty paniki rynkowej lub prowadzić do nieoczekiwanych wahań cen aktywów. Dlatego też niezbędne jest opracowanie mechanizmów monitorowania i kontrolowania działań algorytmów, które będą w stanie reagować w czasie rzeczywistym na potencjalne zagrożenia dla stabilności rynków[135]. W dłuższej perspektywie kluczowym wyzwaniem dla sektora finansowego będzie wskazanie równowagi między wykorzystaniem sztucznej inteligencji a zachowaniem elementu ludzkiego w podejmowaniu decyzji. Podsumowując, wyzwania związane z wykorzystaniem AI w finansach są złożone i wielowymiarowe, obejmując kwestie technologiczne, regulacyjne, organizacyjne. Sektor finansowy stoi przed koniecznością odpowiedzialnego zarządzania tymi wyzwaniami, aby w pełni wykorzystać potencjał sztucznej inteligencji, jednocześnie minimalizując ryzyka i zapewniając zaufanie uczestników rynku. Tylko poprzez zastosowanie zrównoważonego podejścia możliwe będzie skuteczne wdrożenie AI, które przyniesie korzyści instytucjom finansowym, ich klientom oraz społeczeństwu.

[135] Qureshi, N. I., Choudhuri, S. S., Nagamani, Y., Varma, R., & Shah, R. (2024). Ethical Considerations of AI in Financial Services: Privacy, Bias, and Algorithmic Transparency. *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)*, 1–6. DOI: 10.1109/ICKECS61492.2024.10616483

ROZDZIAŁ III. KRÓTKOTERMINOWE SKUTKI CYBERATAKÓW NA RYNKI FINANSOWE

1. Analiza wpływu cyberataków na wartość rynkową przedsiębiorstw

Cyberataki stanowią coraz większe zagrożenie dla przedsiębiorstw, zwłaszcza tych działających na rynkach finansowych, gdzie bezpieczeństwo danych oraz stabilność operacyjna mają kluczowe znaczenie. W obliczu rosnącej liczby incydentów cybernetycznych pojawia się pytanie, w jaki sposób ataki te wpływają na wartość rynkową firm i jakie mechanizmy decydują o skali tej reakcji. Z perspektywy rynków finansowych najważniejszym wskaźnikiem oddziaływania cyberataków na przedsiębiorstwa jest ich wartość rynkowa, która odzwierciedla percepcję inwestorów i reakcję giełdy na dane wydarzenie.[136] Aby dokładnie zbadać te reakcje, wykorzystywana jest najczęściej metoda *event study*, która pozwala na ilościową analizę wpływu konkretnych zdarzeń na ceny akcji oraz kapitalizację rynkową firm. Autor w swoich badaniach wybrał właśnie tę metodę.

Metoda event study

Metoda *event study* polega na identyfikacji wpływu określonego wydarzenia – w tym przypadku cyberataku – na ceny akcji danej spółki w krótkim horyzoncie czasowym. Kluczowym elementem tej metody jest wyznaczenie tzw. okna zdarzenia, czyli przedziału czasowego, w którym analizuje się reakcję rynku na incydent. Standardowe okna zdarzenia obejmują okres od kilku dni przed cyberatakiem do kilku dni po nim (np. -3, +3 dni), co pozwala uwzględnić zarówno początkowe spekulacje inwestorów, jak i późniejsze zmiany wynikające z dalszej analizy skutków ataku. W przypadku bardziej znaczących incydentów, takich jak masowe wycieki danych czy ataki paraliżujące działalność przedsiębiorstwa, okno zdarzenia może być wydłużone, aby uwzględnić długofalowe konsekwencje.

[136] Issayeva, G. K., Zhussipova, E., Aitymbetova, A., Kuralbayeva, A. S., & Abdykulova, D. B. (2024). *The Impact of Cybersecurity Breaches on Firm's Market Value: The Case of the USA.* DOI: 10.51176/1997-9967-2023-4-200-219

Podstawowym wskaźnikiem stosowanym w analizie z wykorzystaniem metody *event study* są nadzwyczajne zwroty (AR – *abnormal returns*), czyli różnica między rzeczywistym zwrotem z akcji a oczekiwanym zwrotem, który zostałby osiągnięty, gdyby cyberatak nie miał miejsca. Oczekiwane zwroty oblicza się na podstawie historycznych danych rynkowych, wykorzystując modele ekonometryczne, takie jak m.in. model rynkowy (*market model*), który uwzględnia współzależność cen akcji z indeksem giełdowym. Popularne modele stosowane w tego typu analizach to także model CAPM (*Capital Asset Pricing Model*) oraz *Fama-French Three-Factor Model*, które pozwalają lepiej kontrolować wpływ czynników rynkowych na ceny akcji. Po wyznaczeniu nadzwyczajnych zwrotów dla poszczególnych dni okna zdarzenia oblicza się skumulowane nadzwyczajne zwroty (CAR – *cumulative abnormal returns*), które pokazują, jak dużą stratę (lub w rzadkich przypadkach zysk) poniosła dana spółka w wyniku cyberataku[137].

Badania wskazują, że średni spadek wartości rynkowej spółek z sektora technologicznego po ujawnieniu cyberataku wynosi od 1,5% do 3,5% w ciągu pierwszych trzech dni po incydencie, przy czym największe straty ponoszą przedsiębiorstwa, których kluczową działalnością jest przetwarzanie danych klientów[138]. Firmy z sektorów takich jak przemysł czy produkcja, które nie są bezpośrednio zależne od infrastruktury cyfrowej, mogą doświadczać mniej dotkliwych reakcji, zwłaszcza jeśli cyberatak nie wpłynął bezpośrednio na ich zdolność do generowania przychodów. Ponadto istotnym czynnikiem wpływającym na skalę reakcji rynków jest sposób, w jaki przedsiębiorstwo komunikuje cyberatak oraz jak wdrażane są środki zaradcze. Firmy, które szybko reagują, przejmując kontrolę nad sytuacją i wdrażając skuteczne strategie naprawcze, mogą zminimalizować skutki rynkowe incydentu, podczas gdy brak przejrzystości i opóźnienia w komunikacji mogą pogłębić negatywną reakcję inwestorów. Przykładem jest atak na firmę Equifax w 2017 roku, gdzie nieudolne zarządzanie kryzysem i opóźniona komunikacja spowodowały, że spółka straciła ponad 4 miliardy dolarów kapitalizacji rynkowej w ciągu dwóch tygodni od ujawnienia ataku[139].

---

[137] Campbell J. Y., Lo A. W., MacKinlay A. C., *The Econometrics of Financial Markets*, Princeton University Press, Princeton 1997, s. 149–180, DOI: 10.1515/9781400830213

[138] Akyildirim E., Conlon T., Corbet S., Hou Y., *HACKED: Understanding the Stock Market Response to Cyberattacks*, *Journal of Economic Behavior & Organization*, Elsevier, Amsterdam 2024, DOI: 10.1016/j.jebo.2024.106423.

[139] Kamiński P., *The Equifax Data Breach and Its Market Impact: A Case-Based Event Study*, *Journal of Risk and Financial Management*, vol. 14, no. 6, MDPI, Basel 2021, art. 277, DOI: 10.3390/jrfm14060277

Warto również zwrócić uwagę na zjawisko tzw. efektu odbicia (*post-breach recovery*), które polega na stopniowym odzyskiwaniu wartości rynkowej przez spółki po pierwszej fazie paniki inwestorów. Badania pokazują, że w przypadku firm, które wdrażają skuteczne strategie naprawcze i zwiększają inwestycje w bezpieczeństwo IT, wartość akcji może stopniowo powracać do poziomu sprzed ataku w ciągu kilku miesięcy. Jednak w przypadku przedsiębiorstw, które nie podejmują działań zaradczych, straty mogą utrzymywać się przez dłuższy czas, prowadząc do spadku zaufania inwestorów i potencjalnych problemów finansowych. Wykorzystanie metody *event study* w badaniu skutków cyberataków jest istotne nie tylko z perspektywy akademickiej, ale także praktycznej. Inwestorzy, menedżerowie oraz regulatorzy mogą dzięki niej lepiej zrozumieć, jakie czynniki decydują o wrażliwości przedsiębiorstw na zagrożenia cybernetyczne oraz jak efektywnie reagować na tego rodzaju incydenty. Analiza krótkoterminowych skutków pozwala również wskazać, które sektory są najbardziej podatne na tego typu wydarzenia i jakie mechanizmy mogą minimalizować ich negatywne konsekwencje. W kolejnych częściach rozdziału zostaną przedstawione konkretne przypadki cyberataków oraz ich wpływ na wartość rynkową przedsiębiorstw, co umożliwi głębsze zrozumienie mechanizmów rynkowych i pozwoli na wyciągnięcie wniosków dotyczących strategii zarządzania ryzykiem cybernetycznym. Badania empiryczne przeprowadzone prze autora pracy zostaną uzupełnione o analizę czynników, które wpływają na różnice w reakcjach rynków w zależności od specyfiki sektora oraz charakterystyki samego ataku. W ten sposób możliwe będzie wskazanie najlepszych praktyk dla firm, które chcą skutecznie minimalizować skutki cyberataków oraz zwiększać odporność swoich systemów finansowych[140].

2. Wybór próby badawczej

Wybór odpowiedniej próby badawczej jest kluczowym etapem analizy z zastosowaniem metody *event study*, ponieważ od tego zależy wiarygodność i reprezentatywność wyników badania. W niniejszej pracy proces selekcji przypadków został zaprojektowany w taki sposób,

[140] Gatzert N., Martin M., *The Impact of Cyber Risks on Capital Markets – An Empirical Event Study*, *European Actuarial Journal*, vol. 12, Springer, Cham 2022, s. 157–185, DOI: 10.1007/s13385-021-00294-

aby umożliwić ocenę krótkoterminowego wpływu cyberataków na wartość rynkową firm notowanych na giełdzie, zgodnie z przyjętą hipotezą: *„Cyberataki mają istotnie negatywny wpływ na krótkoterminową wartość rynkową firm notowanych na giełdzie, co znajduje odzwierciedlenie w ujemnych wartościach skumulowanych nadzwyczajnych zwrotach (CAR) po ujawnieniu incydentu”*. W niniejszym badaniu autor koncentruje się na ogólnym wpływie cyberataków, zamiast uwzględniać różnice sektorowe czy typy ataków. Takie podejście wymaga starannie dobranej, lecz uproszczonej próby, umożliwiającej uchwycenie ogólnych trendów rynkowych. W celu wyboru próby badawczej autor zidentyfikował kryteria wyboru, jak również uzasadnił zakres czasowy okna bazowego oraz zdarzenia, źródła danych giełdowych oraz potencjalne ograniczenia tej selekcji.

Podstawowym kryterium doboru przypadków było *notowanie firmy na giełdzie w momencie ujawnienia cyberataku*. Tylko w odniesieniu do spółek publicznych możliwa jest analiza reakcji rynkowych poprzez dane giełdowe, takie jak ceny akcji i kapitalizacja rynkowa, co jest niezbędne do obliczenia nadzwyczajnych zwrotów (AR) i skumulowanych nadzwyczajnych zwrotów (CAR). Firmy nienotowane zostały wykluczone, ponieważ brak ich publicznego charakteru uniemożliwia zastosowanie metody *event study* w ich przypadku. Wybór ten jest zgodny z literaturą przedmiotu, która podkreśla, że reakcje inwestorów na incydenty kryzysowe, w tym cyberataki, są najlepiej widoczne w krótkoterminowych zmianach notowań giełdowych.[141]

Drugim kryterium była *dostępność precyzyjnych danych dotyczących daty ujawnienia cyberataku*. W metodzie *event study* kluczowe jest ustalenie dnia zero (t=0), czyli momentu, w którym informacja o incydencie stała się publiczna i mogła wpłynąć na decyzje inwestorów. Dlatego wybrano tylko te przypadki, dla których data ujawnienia została jasno udokumentowana w wiarygodnych źródłach, takich jak komunikaty prasowe, raporty firmowe (np. ESPI w Polsce, SEC w USA) lub artykuły w renomowanych mediach (np. Reuters, BBC). Incydenty, co do których informacje były ujawniane stopniowo lub brakowało jednoznacznej daty pierwszej publikacji, zostały wykluczone, aby uniknąć rozproszenia efektu rynkowego w czasie, co mogłoby zaburzyć wyniki analizy. Przykładem dobrze udokumentowanego

[141] Wang, Q., & Ngai, E. (2020). Event study methodology in business research: a bibliometric analysis. *Ind. Manag. Data Syst.*, 120, 1863-1900. https://doi.org/10.1108/IMDS-12-2019-0671.

przypadku jest np. atak na firmę Equifax (EFX) z 7 września 2017 roku, gdzie data ujawnienia została precyzyjnie ustalona na podstawie komunikatu firmy i reakcji mediów.

Trzecim kryterium była *izolacja efektu cyberataku od innych wydarzeń rynkowych*. Aby zapewnić, że obserwowane zmiany w wartości rynkowej wynikają bezpośrednio z ujawnienia incydentu, a nie z nakładających się czynników zewnętrznych, takich jak raporty finansowe, zmiany stóp procentowych czy kryzysy gospodarcze, wybrano przypadki, w których cyberatak był jedynym znaczącym zdarzeniem w oknie zdarzeniowym (-3, +3). Na przykład, jeśli w tym samym okresie firma publikowała wyniki kwartalne lub ogłaszała fuzję, przypadek taki został wykluczony z próby. Takie podejście zwiększyło przejrzystość analizy i pozwoliło przypisać zmiany w AR i CAR wyłącznie badanemu zdarzeniu, co jest zgodne z zaleceniami metodycznymi[142].

Czwartym kryterium była *istotność cyberataku*, definiowana jako jego zdolność do wywołania zauważalnej reakcji rynkowej. W analizie uwzględniono incydenty o znaczącym zasięgu, takie jak masowe wycieki danych, ataki *ransomware* paraliżujące operacje lub inne zdarzenia, które miały potencjalny wpływ na kapitalizację rynkową firmy. Drobne incydenty, takie jak pojedyncze naruszenia bezpieczeństwa bez wyraźnych konsekwencji finansowych zostały pominięte, ponieważ ich wpływ na rynek jest zazwyczaj marginalny i trudny do zmierzenia w krótkim okresie. Przykładem istotnego incydentu jest np. atak na Target (TGT) z 19 grudnia 2013 roku, który doprowadził do wycieku danych 40 milionów kart płatniczych i wywołał spadek akcji o 11% w ciągu miesiąca).

Próba obejmuje *cyberataki z okresu od 1 stycznia 2010 roku do 31 grudnia 2024 roku*, co daje szeroki horyzont czasowy wynoszący 15 lat. Wybór tego zakresu ma kilka uzasadnień.

Po pierwsze, okres ten pokrywa dynamiczny rozwój technologii cyfrowych i rosnące znaczenie cyberbezpieczeństwa w gospodarce globalnej, co pozwala uchwycić ewolucję reakcji rynkowych na cyberataki w różnych warunkach ekonomicznych i technologicznych. Na przykład, w latach 2010-2015 cyberataki były mniej powszechne i często traktowane jako nowość, co mogło prowadzić do bardziej gwałtownych reakcji inwestorów, podczas gdy w

[142] Ullah, S., Zaefarian, G., Ahmed, R., & Kimani, D. (2021). How to apply the event study methodology in STATA: An overview and a step-by-step guide for authors. *Industrial Marketing Management*. https://doi.org/10.1016/J.INDMARMAN.2021.02.004.

latach późniejszych (np. 2020-2024) większa świadomość zagrożeń mogła wpłynąć na bardziej stonowane odpowiedzi rynkowe.

Po drugie, 15-letni zakres umożliwia włączenie różnorodnych przypadków z różnych regionów i giełd (np. NYSE, NASDAQ, TSE), co zwiększa reprezentatywność próby i pozwala na uogólnienie wyników na poziom globalny. Po trzecie, okres ten obejmuje zarówno incydenty sprzed wprowadzenia kluczowych regulacji (np. RODO[143] w 2018 roku), jak i po ich wejściu w życie, co daje możliwość obserwacji, czy zmiany legislacyjne wpłynęły na percepcję ryzyka przez inwestorów. Na przykład, atak na Yahoo (YHOO) z 22 września 2016 roku miał miejsce przed RODO, podczas gdy atak na T-Mobile (TMUS) z 17 sierpnia 2021 roku odbył się w bardziej uregulowanym środowisku, co może wpływać na różnice w kosztach regulacyjnych i reakcjach rynkowych.

Próba badawcza obejmuje 32 przypadki, co stanowi kompromis między wystarczającą mocą statystyczną a praktycznymi ograniczeniami zbierania danych. Literatura dotycząca metody *event study* sugeruje, że minimalna liczba przypadków dla wiarygodnych testów wynosi 30. Wybór 32 przypadków pozwala na uzyskanie istotnych statystycznie wyników przy jednoczesnym zachowaniu możliwości szczegółowej analizy każdego incydentu. Mniejsza próba (np. 10-20 przypadków) mogłaby prowadzić do zbyt dużej wariancji wyników i ograniczonej generalizacji, podczas gdy większa (np. 50-100) wymagałaby zasobów wykraczających poza ramy tej pracy.[144].

Dane do analizy pochodzą z dwóch głównych źródeł: rynkowych i informacyjnych. Dane giełdowe, takie jak dzienne ceny akcji i zwroty indeksów rynkowych (np. S&P 500 dla USA, WIG dla Polski), pozyskano z publicznie dostępnych baz, takich jak m.in. Yahoo Finance, Google Finance oraz Bloomberg Terminal, jeśli były dostępne. Wybór tych źródeł wynika z ich powszechności, dokładności i łatwości dostępu, co jest istotne dla replikowalności badania.

Informacje o cyberatakach pochodzą z renomowanych źródeł medialnych (np. Reuters, BBC, NY Times), raportów firmowych oraz baz danych cyberbezpieczeństwa, takich jak np.

---

[143] Parlament Europejski i Rada Unii Europejskiej, *Rozporządzenie (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO)*, Dz.U. UE L 119 z 4.5.2016, s. 1–88.

[144] Wang, Q., & Ngai, E. (2020). Event study methodology in business research: a bibliometric analysis. *Ind. Manag. Data Syst.*, 120, 1863-1900. https://doi.org/10.1108/IMDS-12-2019-0671.

Verizon Data Breach Investigations Report czy komunikaty CERT. Wybór tych źródeł zapewnia wysoką wiarygodność dat ujawnienia i szczegółów incydentów.

Próba nie została podzielona na sektory ani typy ataków, co odróżnia to badanie od bardziej złożonych analiz sektorowych. Decyzja ta wynika z przyjętej koncepcji uproszczenia – zamiast badać różnice między sektorami (np. finansowym, technologicznym) czy typami incydentów (np. ransomware, wycieki danych), skupiono się na ogólnym wpływie cyberataków na wartość rynkową. Nadmierna segmentacja mogłaby prowadzić do problemu małych próbek w poszczególnych grupach, co utrudniałoby uzyskanie statystycznie istotnych wyników. Poza tym, agregacja danych pozwoliła uniknąć ryzyka stronniczości wyników wynikającej z nieregularnych obserwacji w poszczególnych sektorach. Takie podejście pozwala na uogólnienie wyników i uniknięcie komplikacji związanych z małą liczbą przypadków w każdej podgrupie, co mogłoby osłabić moc statystyczną analizy. Poza tym, badanie uogólnionego wpływu cyberataków pozwala na lepsze odniesienie wyników do szerokiego spektrum organizacji i inwestorów. Wyniki mogą być użyteczne zarówno dla firm, jak i inwestorów instytucjonalnych, którzy operują na szerokim rynku, a nie tylko w wybranych sektorach. .

Próba jest zróżnicowana pod względem geograficznym i rynkowym Ta różnorodność pozwala na ocenę, czy wielkość firmy wpływa na skalę reakcji rynkowej, choć nie jest to formalnie testowane w hipotezie. Proces selekcji nie jest wolny od ograniczeń, które mogą wpłynąć na wyniki. Po pierwsze, wybór 32 przypadków, choć wystarczający dla podstawowej analizy, jest stosunkowo mały w porównaniu z badaniami obejmującymi setki zdarzeń. Może to ograniczyć generalizację wyników na całą populację firm giełdowych. Po drugie, skupienie się na istotnych incydentach wprowadza potencjalne skrzywienie selekcji (selection bias) – pominięto mniej znaczące ataki, które mogłyby wywoływać inne reakcje rynkowe (np. neutralne lub pozytywne w rzadkich przypadkach). Po trzecie, dostępność danych różni się między regionami – w USA i Europie Zachodniej incydenty są lepiej udokumentowane niż w niektórych krajach rozwijających się, co może prowadzić do nadreprezentacji firm z rynków rozwiniętych. Aby zminimalizować te ograniczenia, starano się wybierać przypadki z różnych giełd i okresów, a także weryfikować dane z wielu źródeł. Niemniej jednak, świadomość tych potencjalnych słabości jest kluczowa dla interpretacji wyników i zostanie omówiona w sekcji wniosków.

W kolejnym podrozdziale autor przedstawia okna czasowe i obliczenia AR oraz CAR dla wybranych przypadków, co pozwoli na empiryczną weryfikację wpływu cyberataków na rynki.

3. Opis przypadków cyberataków i wstępna klasyf kacja wpływu na rynki

W niniejszym podrozdziale przedstawiono wybrane przykłady incydentów cybernetycznych, które miały miejsce w ostatnich latach, wraz z ich wstępną klasyfikacją pod kątem rodzaju ataku, sektora gospodarki, skali oddziaływania oraz potencjalnego wpływu na funkcjonowanie rynków finansowych. W tabeli zaprezentowano zestawienie przypadków obejmujących ataki na pojedyncze przedsiębiorstwa. Każdy z opisanych przypadków został scharakteryzowany poprzez identyfikację kluczowych cech, takich jak ujawnienia data zdarzenia, rodzaj wykorzystanego zagrożenia, bezpośrednie skutki dla przedsiębiorstw oraz reakcje rynkowe w postaci zmian wartości akcji. Celem zestawienia jest ukazanie różnorodności form cyberzagrożeń oraz wstępna ocena ich ekonomicznych konsekwencji, co stanowi punkt wyjścia do pogłębionej analizy empirycznej w kolejnych rozdziałach pracy.

Tabela 1. Szczegółowe opisy cyberataków wybranych przypadków .

Nazwa firmy i krótka charakterystyka (Ticker)	Rodzaj incydentu	Opis incydentu
Adobe (ADBE) – Firma oprogramowania, NASDAQ, Photoshop.	Wyciek danych	3 października 2013 r. Adobe ujawniło włamanie, które objęło dane klientów (m.in. identyfikatory, e-maile, zaszyfrowane hasła i podpowiedzi haseł) oraz kody źródłowe ważnych produktów (ColdFusion, Acrobat/Reader; doniesienia wskazywały także na częściowy dostęp do kodu Photoshopa). W kolejnych tygodniach skala aktywnych kont objętych naruszeniem została potwierdzona na ok. 38 mln. Wyciek kodu źródłowego zwrócił uwagę na ryzyka „długiego pobytu" napastników w sieci, niedostateczną segmentację środowisk developerskich oraz potrzebę ścisłego zarządzania prawami dostępu do repozytoriów. Incydent stał się w branży oprogramowania punktem odniesienia dla polityk ochrony kodu, przeglądów uprawnień i obowiązkowych przeglądów tajności podpowiedzi haseł[145].
Anthem (ELV) – Ubezpieczyciel zdrowotny, NYSE.	Wyciek danych	Kampania phishingowa umożliwiła atakującym dostęp do środowisk Anthem i kradzież danych osobowych 78,8 mln osób (imię, nazwisko, SSN, data urodzenia, adres), co ogłoszono 4 lutego 2015 r. Firma deklarowała, że nie obejmowało to historii medycznych ani danych kart. Sprawa nagłośniła problem braku szyfrowania PII „w spoczynku" w dużych

[145] B. Krebs, *Adobe To Announce Source Code, Customer Data Breach*, KrebsOnSecurity, 3.10.2013, https://krebsonsecurity.com/2013/10/adobe-to-announce-source-code-customer-data-breach/

		organizacjach ochrony zdrowia i zakończyła się pozwami zbiorowymi oraz ugodami regulacyjnymi w wielu stanach. Przypadek do dziś cytowany jest jako precedens wymuszający modernizację kontroli dostępu, MFA i monitoringu anomalii w sektorze ubezpieczeń zdrowotnych.[146].
Aon (AON) – Ubezpieczenia, NYSE, usługi brokerskie.	Nieokreślony incydent	25 II 2022 r. Aon wykrył „incydent cybernetyczny" oddziałujący na ograniczoną liczbę systemów. W zgłoszeniu Form 8-K (28 II) spółka nie potwierdziła ransomware, podkreślając brak szyfrowania danych i ograniczony wpływ operacyjny. Firma uruchomiła procedury reagowania, współpracując z zewnętrznymi specjalistami i organami ścigania. Przypadek ten bywa mylony z atakami szyfrującymi, jednak komunikacja Aon wskazuje na kontrolowany charakter zdarzenia i zarządczo-compliance'owe znaczenie szybkich raportów giełdowych.[147].
Boeing (BA) – Producent lotniczy, NYSE.	Ransomware	28–29 III 2018 r. Boeing potwierdził ograniczoną infekcję związaną z WannaCry, zaznaczając, że incydent dotyczył niewielkiej liczby maszyn i nie miał wpływu na produkcję czy dostawy. Publicznie zdementowano doniesienia o zakłóceniach na liniach 737/777. Wydarzenie uwypukliło znaczenie separacji środowisk IT/OT, aktualizacji systemów

[146] California Dept. of Insurance, *Consumer information on Anthem breach*, 2015, https://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm
[147] Cimpanu, C. (2022, February 28). *Insurance giant Aon hit by a cyberattack over the weekend*. BleepingComputer. Link do artykułu.

		starszej generacji oraz szybkiej i wyważonej komunikacji, aby przeciwdziałać panice rynkowej w sektorze lotniczym.[148].
British Airways (IAG) – Linie lotnicze, LSE via IAG.	Wyciek danych	Atak „Magecart" na kod front-endu BA (22 VI–5 IX 2018) przekierowywał dane płatnicze klientów na serwer kontrolowany przez przestępców. Ujawniono narażenie ~380 tys. kart i ok. 500 tys. klientów; dochodzenie ICO wykazało braki w kontrolach, testach i segmentacji. Ostateczna kara ICO: £20 mln (2020; niżej niż pierwotna propozycja £183 mln). Sprawa stała się klasycznym case study ataków skimmingowych na ścieżkę płatniczą i argumentem za CSP, SRI i ciągłym testowaniem zmian JS.[149][150].
Capital One (COF) – Bank, NYSE, usługi finansowe.	Wyciek danych	29 VII 2019 r. ogłoszono, że była pracownica firmy technologicznej Paige Thompson wykorzystała błędną konfigurację WAF/zapory w środowisku AWS, uzyskując dostęp do zbiorów S3. Dotyczyło to ~106 mln osób (m.in. 140 tys. SSN i 80 tys. numerów rachunków; część kanadyjska). Thompson chwaliła się w serwisach i na GitHubie, co ułatwiło identyfikację i zatrzymanie. Incydent uwypuklił model „shared responsibility" i konieczność

[148] Ferguson, S. (2018, March 29). *WannaCry Ransomware Hits Boeing, but Company Claims It's Contained*. Dark Reading. https://www.darkreading.com/application-security/wannacry-ransomware-hits-boeing-but-company-claims-it-s-contained

[149] ICO (final), *BA fined £20m*, 2020 (omów.), https://www.gdprregister.eu/news/british-airways-fine/

[150] Aljaidi, M. (2023). A Comprehensive Technical Analysis of URL Redirect Attacks: A Case Study of British Airways Data Breach. *2023 24th International Arab Conference on Information Technology (ACIT)*, 1-5. https://doi.org/10.1109/ACIT58888.2023.10453784.

		automatycznych kontroli konfiguracji IaC, a także threat-modeling interfejsów metadanych.[151]
Cognizant (CTSH) – Firma IT, NASDAQ, usługi tech.	Ransomware	18 IV 2020 r. Cognizant oficjalnie potwierdził atak Maze, który spowodował zakłócenia usług u części klientów i exfiltrację danych. Spółka musiała odbudowywać środowiska, co pokazało, jak duży efekt kaskadowy może mieć ransomware u kluczowego dostawcy usług IT. Przypadek przyspieszył dyskusję o due diligence usług zarządzanych, segmentacji tenantów i przejrzystości komunikacji kryzysowej.[152].
Clorox Company (CLX) –producent środków czystości i artykułów gospodarstwa domowego, NYSE.	Ransomware	Atak ransomware na Clorox został ujawniony 14 sierpnia 2023 roku. Cyberprzestępcy, prawdopodobnie z grupy ALPHV/BlackCat, uzyskali dostęp do wewnętrznej sieci korporacyjnej, paraliżując część systemów produkcyjnych i logistycznych. Firma musiała przejść na ręczne przetwarzanie zamówień, co doprowadziło do znacznych zakłóceń w łańcuchu dostaw oraz spadku efektywności operacyjnej. W komunikacie prasowym Clorox potwierdził, że skutki incydentu wpłyną na wyniki finansowe IV kwartału 2023 roku.

[151] S. Khan i in., *A Systematic Analysis of the Capital One Data Breach*, *ACM Digital Threats* 2022, https://dl.acm.org/doi/full/10.1145/3546068
[152] Cognizant, *Security Incident Update* (komunikat), 18.04.2020, https://news.cognizant.com/2020-04-18-cognizant-security-update

		Według analizy serwisu Bloomberg Cybersecurity Insights, pełne przywrócenie infrastruktury zajęło kilka tygodni[153].
Delta Airlines (DAL) – Linie lotnicze, NYSE.	Wyciek danych	W wyniku kompromitacji systemu płatności u dostawcy [24]7.ai (26 IX–12 X 2017) potencjalnie narażono dane kart „kilkuset tysięcy" klientów Delty; sama linia została o incydencie poinformowana dopiero w 2018 r., co wymusiło dodatkowe powiadomienia i działania naprawcze. Wydarzenie jest wzorcowym przykładem ryzyka łańcucha dostaw w sprzedaży online linii lotniczych i znaczenia kontraktowych wymogów bezpieczeństwa wobec vendorów[154][155].
Deutsche Telekom (DTE) – Operator, FWB.	Atak DDoS	Atak Mirai, ujawniony 28 listopada 2016 roku, Hakerzy wyłączyli 900 tysięcy routerów klientów w Niemczech na kilka godzin. Brak zabezpieczeń IoT umożliwił masowy atak,

[153] Scimeca, D. (2023, October 5). *Updated: Clorox cyberattack cost $356 million*. *IndustryWeek*. Retrieved from https://www.industryweek.com/technology-and-iiot/article/21274431/the-clorox-co-recovers-from-severe-cyberattack

[154] *TIME*, *Data Breach at [24]7.ai may have hit Delta*, 05.04.2018, https://time.com/5230288/delta-sears-data-breach-credit-cards/

[155] Freedman, L. F. (2019, August 14). *Delta Sues Vendor for Causing Data Breach*. The National Law Review. Link do artykułu

		zakłócając usługi internetowe i telefoniczne, co wywołało krytykę i konieczność modernizacji sieci operatora[156].
eBay (EBAY) – Platforma e-commerce, NASDAQ, aukcje online.	Wyciek danych	Atak trwał od lutego do maja 2014 roku, ujawniony 21 maja 2014 roku. Hakerzy wykorzystując metodę phishingu skradli dane logowania pracowników, umożliwiając dostęp do danych 145 milionów użytkowników – e-maile, hasła. eBay wymusił zmianę haseł, ale opóźniona komunikacja wywołała krytykę i podważyła zaufanie klientów do platformy[157][158].
Equifax (EFX) – Agencja kredytowa, NYSE, lider danych kredytowych.	Wyciek danych	Atak trwał od maja do lipca 2017 roku i został ujawniony 7 września 2017 roku. Hakerzy wykorzystali lukę w oprogramowaniu Apache Struts (CVE-2017-5638), której firma nie zniwelowała mimo dostępnej aktualizacji, kradnąc dane 147 milionów klientów, w tym numery SSN, daty urodzenia i dane finansowe. Firma Equifax wykryła naruszenie po 76 dniach z powodu słabego monitoringu sieci, co wywołało krytykę za opóźnioną reakcję i brak przejrzystości. Incydent doprowadził do śledztw organów ścigania i masowych pozwów klientów, ujawniając poważne braki w zabezpieczeniach firmy[159].

[156] Gallopeni, G., Rodrigues, B., Franco, M., & Stiller, B. (2020). A Practical Analysis on Mirai Botnet Traffic. *2020 IFIP Networking Conference (Networking)*, 667-668. https://doi.org/10.5281/ZENODO.3966899.

[157] BankInfoSecurity, *eBay Breach: 145 Million Users Notified*, 21.05.2014, https://www.bankinfosecurity.com/ebay-a-6858
[158] Kolevski, D., Michael, K., Abbas, R., & Freeman, M. (2021). Cloud Data Breach Disclosures: the Consumer and their Personally Identifiable Information (PII)?. *2021 IEEE Conference on Norbert Wiener in the 21st Century (21CW)*, 1-9. https://doi.org/10.1109/21CW48944.2021.9532579.
[159] Glenn, A. (2018). Equifax: Anatomy of a Security Breach. .

FedEx (FDX) – Firma logistyczna, NYSE, dostawy.	Ransomware	Czerwiec 2017: spółka zależna TNT Express została mocno dotknięta przez NotPetya (rozprzestrzeniony m.in. via ukraińskie oprogramowanie podatkowe). FedEx raportował istotne zakłócenia operacyjne u TNT oraz koszty liczonych setkami milionów USD w kolejnych okresach sprawozdawczych. Incydent unaocznił systemowe ryzyko geopolitycznych kampanii destrukcyjnych oraz potrzebę segmentacji i izolacji regionalnych środowisk IT.[160].
First American (FAF) – Ubezpieczenia, NYSE.	Wyciek danych	24 maja 2019 r. ujawniono, że serwis First American bez autoryzacji udostępniał sekwencyjnie linkowane dokumenty (od 2003 r.), co skutkowało publiczną ekspozycją ~885 mln plików (dane finansowe, hipoteczne, identyfikacyjne). Zdarzenie było efektem błędu aplikacyjnego, a nie klasycznego „włamania". Sprawą zainteresowała się SEC. Incydent stał się ważnym przykładem ryzyka „insecure direct object reference" i testów bezpieczeństwa w serwisach dokumentowych[161].
Garmin (GRMN)	Ransomware	23–27 VII 2020: atak WastedLocker sparaliżował usługi (Garmin Connect, część usług lotniczych), centra obsługi i niektóre linie produkcyjne w Azji. Media szeroko informowały o żądaniu ~10 mln USD i prawdopodobnej płatności (niepotwierdzone oficjalnie), a

[160] Jasper, S. (2019). *North Korea's Cyberspace Aggression*. *International Journal of Intelligence and CounterIntelligence, 32*(2), 194-198.

[161] B. Krebs, *First American… leaked hundreds of millions of records*, 24.05.2019, https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

– Producent wearable, NASDAQ.		przywracanie systemów wiązano z użyciem klucza deszyfrującego. Case pokazał kruchość usług chmurowych i integracji z IoT/urządzeniami końcowymi oraz potrzebę rozdzielenia środowisk krytycznych od usług konsumenckich.[162].
Home Depot (HD) – Sieć remontowa, NYSE, sprzedaż budowlana.	Wyciek danych	IV–IX 2014 r. napastnicy, używając poświadczeń dostawcy, zainstalowali malware na terminalach POS Home Depot, kradnąc dane ~56 mln kart. Dodatkowo wykradziono ~53 mln adresów e-mail. Sprawa zakończyła się m.in. ugodą generalną $17,5 mln z prokuratorami generalnymi stanów. Przypdek posłużył do promocji EMV/tokenizacji i segmentacji sieci sklepów.[163].
JPMorgan Chase (JPM) – Bank inwestycyjny, NYSE.	Wyciek danych	W 2014 r. bank ujawnił naruszenie dotyczące 76 mln gospodarstw domowych i 7 mln firm; dotyczyło głównie danych kontaktowych (bez haseł i numerów kont). Wydarzenie uruchomiło inwestycje w hardening dostępu zewnętrznego i segmentację sieci bankowych oraz przeprojektowanie procesów monitoringu. Incydent, choć bez danych finansowych, miał duże znaczenie reputacyjne i regulacyjne.[164].

[162] (2020). Garmin among hardest hit in major wave of ransomware attacks. *Computer Fraud & Security*, 2020, 1 - 3. https://doi.org/10.1016/s1361-3723(20)30079-8.
[163] Hoehle, H., Wei, J., Schuetz, S., & Venkatesh, V. (2021). User compensation as a data breach recovery action: a methodological replication and investigation of generalizability based on the Home Depot breach. *Internet Res.*, 31, 765-781. https://doi.org/10.1108/INTR-02-2020-0105.
[164] Murphy, M. (2014). JPMorgan Data Breach Involves Information on 76 Million Households, 7 Million Small Businesses. .

Lockheed Martin (LMT) – Firma obronna, NYSE.	Atak hakerski	Atak ujawniony 28 maja 2011 roku. Atakujący wykorzystali kompromitację RSA SecurID, co skłoniło Lockheeda do natychmiastowych blokad i wymiany tokenów. Wydarzenie, szeroko komentowane w branży obronnej, podkreśliło ryzyka łańcucha dostaw 2FA oraz sens wdrożenia koncepcji Cyber Kill Chain w praktyce detekcji/reakcji. Incydent miał znaczenie systemowe dla wszystkich użytkowników SecurID (wymiana tokenów u wielu kontrahentów)[165][166].
Maersk (MAERSK-B) – Firma logistyczna, OMX Copenhagen.	Ransomware	Czerwiec 2017: NotPetya sparaliżowała IT Maerska, co wymagało odbudowy ~45 tys. PC, 4 tys. serwerów i ~2,5 tys. aplikacji w ~10 dni. Szacowane koszty: $250–300 mln. Zakłócenia dotyczyły m.in. ~76 terminali portowych. Case uznawany jest za archetyp odporności i odtwarzania w globalnej logistyce – z silnym naciskiem na segmentację stref/poziomów, kopie offline i „immutable backups".[167][168].

[165] Defense One, *RSA verifies its tokens played role…*, 07.06.2011, https://www.defenseone.com/defense-systems/2011/06/rsa-verifies-its-tokens-played-role-in-lockheed-cyberattack/

[166] Kesan, J., & Hayes, C. (2011). Self Defense in Cyberspace: Law and Policy. .

[167] WIRED, *The Untold Story of NotPetya…*, 22.08.2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[168] Kaila, U., & Nyman, L. (2018). Information Security Best Practices: First Steps for Startups and SMEs. *Technology Innovation Management Review*. https://doi.org/10.22215/TIMREVIEW/1198.

Marriott (MAR) – Sieć hotelowa, NASDAQ, marka Starwood.	Wyciek danych	Atak trwał od 2014 roku, ujawniony 30 listopada 2018 roku. Hakerzy wykorzystali lukę w systemie Starwood, kradnąc dane 500 milionów gości – nazwiska, numery paszportów, dane kart. Marriott po przejęciu Starwood w 2016 nie zintegrował zabezpieczeń, co umożliwiło długotrwałe naruszenie. Opóźniona reakcja wywołała krytykę i śledztwa regulatorów[169][170].
Meta (META) – Sieć społecznościowa, NASDAQ, media online.	Wyciek danych	Atak ujawniony 28 września 2018 roku. Luka w funkcji „View As" umożliwiła kradzież tokenów dostępu do 50 milionów kont. Firma zresetowała tokeny i powiadomiła o ataku użytkowników, ale incydent po skandalu Cambridge Analytica podważył zaufanie do polityki bezpieczeństwa firmy, wywołując reakcję organów rządowych[171].
MGM Resorts (MGM) – Sieć kasyn, NYSE.	Wyciek danych	Atak ujawniony 19 lutego 2020 roku. Hakerzy w 2019 roku skradli dane 10,6 miliona gości – nazwiska, paszporty – publikując je w dark webie. Firma nie wykryła wycieku przez miesiące, co wywołało obawy o bezpieczeństwo informatyczne w sektorze hotelarskim i krytykę opinii publicznej w zakresie zarządzania danymi[172].

[169] Hotel Law Blog, *Lessons from Marriott's £99m GDPR fine*, 07.08.2019, https://hotellaw.jmbm.com/cybersecurity-lawyer-marriotts-123-million-gdpr-fine.html
[170] Bharadwaj, Y., Bhageerath, Y., & Prof., Y. (2019). Cyber Security, Challenges, Some Practical Solutions. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. https://doi.org/10.32628/CSEIT19519.
[171] Foecking, N., Wang, M., & Huynh, T. (2021). How do investors react to the data breaches news? Empirical evidence from Facebook Inc. during the years 2016–2019. *Technology in Society*. https://doi.org/10.1016/j.techsoc.2021.101717.
[172] Goldstein, M. (2020, February 20). *MGM Resorts data breach exposes personal info of 10.6 million guests*. Forbes. Link do artykułu.

Norsk Hydro (NHY) – Producent aluminium, OSE.	Ransomware	Atak LockerGoga, ujawniony 19 marca 2019 roku, Hakerzy zaszyfrowali systemy, zatrzymując prace w zakładach w Europie i USA. Firma przeszła na tryb manualny, ale brak backupów zwiększył koszty. Incydent ujawnił słabości w infrastrukturze informatycznej w firmach związanych z przemysłem[173].
PepsiCo (PEP) – Producent spożywczy, NASDAQ.	Wyciek danych	Atak miał miejsce w grudniu 2022 roku; ujawniony 20 stycznia 2023 roku. Hakerzy skradli dane pracowników spółki podległej PepsiCo – SSN, dane finansowe – z systemów HR. PepsiCo potwierdziło incydent po śledztwie, ujawniając słabe zabezpieczenia sieci korporacyjnych i wywołując reakcję regulatorów[174].
Quest Diagnostics (DGX) – Firma medyczna, NYSE[175].	Wyciek danych	3 czerwca 2019 Quest potwierdził, że dostawca windykacji AMCA padł ofiarą naruszenia, obejmującego ~11,9 mln pacjentów (dane osobowe, finansowe oraz część medycznych – bez wyników badań). Incydent dotyczył łańcucha podwykonawców i stał się głośnym przykładem ryzyk vendorowych w ochronie zdrowia[176].

[173] WIRED, *Norsk Hydro cyber attack is about money, not war*, 20.03.2019, https://www.wired.com/story/norsk-hydro-cyber-attack

[174] HALOCK Security Labs. (2023, February 10). *Pepsi Cola bottler falls victim to a data breach*. Retrieved from https://www.halock.com/pepsi-cola-bottler-falls-victim-to-a-data-breach.

[175] Dellinger, A. J. (2019, May 26). *Understanding the First American Financial data leak: How did it happen and what does it mean?* Forbes. Link do artykułu.

[176] EC (8-K), *Quest Diagnostics Statement on the AMCA Data Security Incident*, 03.06.2019, https://www.sec.gov/.../ss138857_8k.htm

SolarWinds (SWI) – Firma IT, NYSE, oprogramowanie.	Atak na łańcuch dostaw	Atak miał miejsce w marcu 2020; ujawniony 13 grudnia 2020 roku. Hakerzy z APT29 (Rosja) wprowadzili malware Sunburst do aktualizacji Orion, infekując tysiące firm i instytucji. Atak, niewykryty przez miesiące, ujawnił słabości łańcuchów dostaw IT i wywołał globalny kryzys zaufania[177].
Target (TGT) – Sieć handlowa, NYSE, sprzedaż detaliczna.	Wyciek danych	Atak trwał od 27 listopada do 15 grudnia 2013 roku, ujawniony 19 grudnia 2013 roku. Hakerzy uzyskali dostęp do danych firmy przez dostawcę HVAC, instalując malware w terminalach POS, kradnąc dane 40 milionów kart i dane osobowe 70 milionów klientów. Incydent miał miejsce w okresie świątecznym, zwiększając straty sprzedaży. Firma nie stosowała odpowiednich zabezpieczeń, co wywołało krytykę i pozwy, ujawniając słabości w zarządzaniu cyberbezpieczeństwem**[178]**.
Tesla (TSLA) – Producent aut, NASDAQ, innowacje.	Kryptojacking	Atak ujawniony 20 lutego 2018 roku. Hakerzy włamali się do chmury Kubernetes, kopiąc kryptowaluty Monero. Firma nie zabezpieczyła odpowiednio systemu informatycznego, ale atak na szczęście nie wpłynął na produkcję aut. Incydent ujawnił podatności chmurowe i wywołał szybką reakcję firmy[179][180].

[177] Dias, T., Coco, A., & Van Benthem, T. (2022). Illegal: The SolarWinds Hack under International Law. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4174397.
[178] Plachkinova, M., & Maurer, C. (2018). Teaching Case: Security Breach at Target. *J. Inf. Syst. Educ.*, 29, 11-20.

[179] WIRED, *Hackers Enlisted Tesla's Cloud to Mine Cryptocurrency*, 20.02.2018, https://www.wired.com/story/cryptojacking-tesla-amazon-cloud/
[180] Meland, P., Johansen, B., & Sindre, G. (2019). An Experimental Analysis of Cryptojacking Attacks. , 155-170. https://doi.org/10.1007/978-3-030-35055-0_10.

T-Mobile (TMUS) – Operator telekomunikacyjny, NASDAQ.	Wyciek danych	Atak z sierpnia 2021 roku; ujawniony został 17 sierpnia 2021 roku. Haker John Binns wykorzystał lukę w API, kradnąc dane 47 milionów klientów – numery telefonów, adresy, SSN. Słabe zabezpieczenia T-Mobile wywołały pozwy i krytykę, ujawniając brak przygotowania na masowe naruszenia[181].
Toyota (TM) – Producent aut, NYSE.	Atak na łańcuch dostaw	Atak ujawniony 1 marca 2022 roku. W incydentu u dostawcy Kojima Industries Toyota wstrzymała 28 linii w 14 fabrykach w Japonii na jeden dzień. Choć nie potwierdzono szerokiej kradzieży danych, wpływ na produkcję był natychmiastowy i pokazał, że cyberincydent u jednego dostawcy może zatrzymać giganta produkcyjnego. Wzmocniono audyty vendorów i segmentację sieci produkcyjnych[182].
Under Armour (UAA) – Producent odzieży, NYSE.	Wyciek danych	Atak miał miejsce w lutym 2018 roku; ujawniony 29 marca 2018 roku. Hakerzy skradli dane 150 milionów użytkowników MyFitnessPal – e-maile, hasła (bcrypt). Wyciek został

[181] Faircloth, C., Hartzell, G., Callahan, N., & Bhunia, S. (2022). A Study on Brute Force Attack on T-Mobile Leading to SIM-Hijacking and Identity-Theft. *2022 IEEE World AI IoT Congress (AIIoT)*, 501-507. https://doi.org/10.1109/aiiot54504.2022.9817175.

[182] DARKReading, *Toyota halts production after suspected supply chain attack*, 01.03.2022, https://www.darkreading.com/cyberattacks-data-breaches/toyota-halts-production-after-suspected-supply-chain-attack

		spowodowany poprzez brak szyfrowania, co wywołało krytykę klientów i opinii publicznej i złożenie wielu pozwów, ujawniając słabości w zarządzaniu aplikacjami firmy[183].
Walgreens (WBA) – Sieć aptek, NASDAQ.	Wyciek danych	Atak ujawniony 10 października 2020 roku. Hakerzy od dostawcy Accellion FTA (2019-2020) skradli dane pacjentów – recepty, dane osobowe. Firma Walgreens nie była bezpośrednio zaatakowana, ale ucierpiała na reputacji, gdyż wymagało to powiadomienia klientów i wprowadzenia działań naprawczych[184].

Źródło: opracowanie własne.

[183] Torres, K., Stevenson, A., & Hicks, J. (2021). Case Study: Under Armour Hack. In D. Sen & R. Ahmed (Eds.), *Privacy Concerns Surrounding Personal Information Sharing on Health and Fitness Mobile Apps* (pp. 145-162). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-7998-3487-8.ch006
[184] HIPAA Journal, *Flaw in Walgreens Mobile App…*, 04.03.2020, https://www.hipaajournal.com/flaw-walgreens-mobile-app-secure-messaging-feature-exposed-phi/

4. Określenie okna bazowego i okna zdarzenia oraz podział na kategorie wpływu

Okno bazowe to okres, w którym szacowane są parametry modelu służącego do przewidywania normalnych zwrotów akcji, czyli takich, jakie miałyby miejsce, gdyby cyberatak nie został ujawniony. W niniejszym badaniu wykorzystano **model rynkowy** (*market model*), który zakłada liniową zależność zwrotów danej akcji od zwrotów indeksu rynkowego. Aby oszacowanie parametrów modelu było wiarygodne, okno bazowe powinno być wystarczająco długie, ale jednocześnie wolne od wpływu innych znaczących zdarzeń, które mogłyby zakłócić zachowanie akcji.

W literaturze dotyczącej metody *event study* długość okna bazowego zazwyczaj mieści się w przedziale od 100 do 250 dni obrotowych przed oknem zdarzenia. W niniejszej analizie przyjęto okno bazowe obejmujące 120 dni obrotowych poprzedzających okno zdarzenia. Wybór ten stanowi kompromis między dążeniem do precyzyjnego oszacowania parametrów a ograniczeniami wynikającymi z dostępności danych. Ponadto, długość okna bazowego została dostosowana do specyfiki analizowanego rynku finansowego, uwzględniając jego zmienność i strukturę.Okno bazowe kończy się na 5 dni obrotowych przed dniem ujawnienia cyberataku (t = -5), gdzie t = 0 oznacza dzień ujawnienia. Taki odstęp pozwala zminimalizować ryzyko wpływu przecieków informacji lub spekulacji rynkowych na szacunki parametrów modelu.

Okno zdarzenia to okres, w którym analizowana jest reakcja rynku na ujawnienie cyberataku. Obejmuje ono dni przed, w trakcie i po incydencie, co pozwala uchwycić zarówno ewentualne przecieki informacji, jak i krótkoterminowe skutki zdarzenia. W niniejszej analizie przyjęto okno zdarzenia obejmujące 7 dni obrotowych: od t = -3 do t = +3, gdzie t = 0 to dzień ujawnienia cyberataku.

Taki zakres okna zdarzenia został wybrany z następujących powodów:

- **Dni przed ujawnieniem (t = -3 do t = -1)**: Umożliwiają analizę potencjalnych przecieków informacji lub spekulacji rynkowych, które mogły wpłynąć na ceny akcji jeszcze przed oficjalnym ogłoszeniem.

- **Dzień ujawnienia (t = 0)**: Pozwala zaobserwować natychmiastową reakcję rynku na informację o cyberataku.
- **Dni po ujawnieniu (t = +1 do t = +3)**: Umożliwiają ocenę krótkoterminowych skutków, uwzględniając czas potrzebny inwestorom na pełne przetworzenie informacji.

Wybór okna zdarzenia od t = -3 do t = +3 jest zgodny z praktyką stosowaną w badaniach wpływu zdarzeń kryzysowych na rynki finansowe.

W kolejnych częściach pracy autor przedstawia wyniki analizy CAR dla poszczególnych przypadków z uwzględnieniem tej klasyfikacji, co pozwala na wyciągnięcie wniosków o krótkoterminowym wpływie cyberataków na rynki finansowe.

Określenie okna bazowego i okna zdarzenia jest fundamentem analizy wpływu cyberataków na wartość rynkową firm z wykorzystaniem metody *event study*. Okno bazowe, obejmujące 120 dni przed zdarzeniem, umożliwia oszacowanie normalnych zwrotów akcji, natomiast okno zdarzenia (-3, +3) pozwala uchwycić krótkoterminową reakcję rynku na ujawnienie cyberataku. Podział na kategorie wpływu na podstawie CAR dostarcza dodatkowej warstwy analitycznej, ułatwiając zrozumienie zróżnicowanego oddziaływania cyberataków na przedsiębiorstwa notowane na giełdzie. Wyniki tej analizy mogą stanowić podstawę do dalszych badań nad mechanizmami reakcji rynku na tego typu zdarzenia.

5. Analiza i interpretacja wpływu cyberataków na wartość rynkową f rm za pomocą metody event study

Autor przeprowadził analizę krótkoterminowego wpływu cyberataków na wartość rynkową firm notowanych na giełdzie, wykorzystując metodę *event study*. Analiza bazuje na danych zebranych dla **32 przypadków cyberataków**, które spełniają kryteria wyboru opisane w rozdziale III, takie jak:

- notowanie na giełdzie,
- precyzyjna data ujawnienia incydentu,

- istotność zdarzenia.

Celem badania jest obliczenie:

- **oczekiwanych zwrotów akcji**,
- **nadzwyczajnych zwrotów (AR)**,
- **skumulowanych nadzwyczajnych zwrotów (CAR)**

w **oknie zdarzenia**, a następnie przeprowadzenie analizy statystycznej w celu zweryfikowania hipotezy wskazującej, że:

Cyberataki mają istotnie negatywny wpływ na krótkoterminową wartość rynkową firm notowanych na giełdzie, co znajduje odzwierciedlenie w ujemnych wartościach skumulowanych nadzwyczajnych zwrotów (CAR) po ujawnieniu incydentu.

Oczekiwane zwroty akcji obliczono przy użyciu **modelu rynkowego (market model)**, który zakłada liniową zależność między zwrotami danej akcji a zwrotami indeksu rynkowego. Model ten jest powszechnie stosowany w badaniach ***event study*** ze względu na swoją **prostotę i skuteczność w szacowaniu normalnych zwrotów**.

Dla każdej firmy i, model rynkowy ma postać:

$$\boldsymbol{R_{it} = \alpha_i + \beta_i R_{mt} + \in_{it}}$$

gdzie:

- R_{it} – zwrot akcji firmy i w dniu t,
- R_{mt}– zwrot indeksu rynkowego w dniu t,
- α_i, β_i – parametry modelu specyficzne dla firmy i,
- $\in_{it}$ – błąd losowy.

Parametry α_i, β_i oszacowano metodą **regresji liniowej** na podstawie danych z **okna bazowego**, obejmującego **120 dni obrotowych** od **t =−124t** do **t=−5t**

gdzie **t=0** to dzień ujawnienia cyberataku.

Dla każdego dnia t w **oknie zdarzenia** (t=−3 do t=+3), oczekiwany zwrot $E(R_{it})$

obliczono jako:

$$\boldsymbol{E(R_{it}) = \widehat{\alpha_i} + \widehat{\beta_i}\, R_{mt}}$$

gdzie:

- $\widehat{\alpha_i}$ $\boldsymbol{i}$ $\widehat{\beta_i}$to oszacowane parametry modelu.

Wartości $\boldsymbol{R_{mt}}$ pochodziły z odpowiednich **indeksów rynkowych** (np. **S&P 500** dla firm z NYSE/NASDAQ), dostosowanych do daty zdarzenia każdej firmy.

Nadzwyczajne zwroty (AR) dla każdego dnia t w oknie zdarzenia obliczono jako różnicę między rzeczywistym zwrotem akcji R_{it} a oczekiwanym zwrotem $E(R_{it})$

$$\boldsymbol{AR_{it} = R_{it} - E(R_{it})}$$

Nadzwyczajne zwroty reprezentują część zwrotu akcji, **która nie jest wyjaśniona przez ogólne zachowanie rynku**, a tym samym może być przypisana do ujawnienia cyberataku.

Aby ocenić **łączny wpływ cyberataku** na wartość rynkową firmy w całym **oknie zdarzenia** (t= −3t do t=+ 3), obliczono **skumulowane nadzwyczajne zwroty (CAR)** według wzoru:

$$\boldsymbol{CAR_i = \sum_{t=-3}^{t=3} AR_{it}}$$

Celem analizy statystycznej było zweryfikowanie, czy średni CAR dla całej próby jest **istotnie ujemny**, co potwierdzałoby hipotezę o negatywnym wpływie cyberataków na wartość rynkową firm.

Tabela 2 przedstawia wyniki analizy skumulowanych nadzwyczajnych zwrotów (CAR) i nadzwyczajnych zwrotów (AR) dla analizowanych firm.

Tabela 2. Wyniki analizy skumulowanych nadzwyczajnych zwrotów (CAR) i nadzwyczajnych zwrotów (AR).

Nazwa firmy	Data okno bazowe od	Data okno bazowe do	Data okno zdarzenia od	Data okno zdarzenia do	CAR(-3,+3)
Equifax	23.03.2017	31.08.2017	04.09.2017	12.09.2017	-19,38%
Target	04.07.2013	12.12.2013	16.12.2013	24.12.2013	-2,31%
Marriott	15.06.2018	23.11.2018	27.11.2018	05.12.2018	-5,72%
Capital One	11.02.2019	22.07.2019	24.07.2019	01.08.2019	-0,88%
Home Depot	24.03.2014	01.09.2014	03.09.2014	11.09.2014	-2,55%
eBay	04.12.2013	14.05.2014	16.05.2014	26.05.2014	-0,14%
Meta	13.04.2018	21.09.2018	25.09.2018	03.10.2018	-1,23%
JPMorgan Chase	17.04.2014	25.09.2014	29.09.2014	07.10.2014	1,04%
Anthem	20.08.2014	28.01.2015	30.01.2015	09.02.2015	-4,19%
British Airways	22.03.2018	30.08.2018	03.09.2018	11.09.2018	-8,19%
T-Mobile	02.03.2021	10.08.2021	12.08.2021	20.08.2021	-2,11%
SolarWinds	29.06.2020	07.12.2020	09.12.2020	16.12.2020	-26,10%
FedEx	25.11.2016	05.05.2017	09.05.2017	17.05.2017	1,73%
Maersk	10.01.2017	20.06.2017	22.06.2017	30.06.2017	6,62%
Adobe	18.04.2013	26.09.2013	30.09.2013	08.10.2013	-2,75%
Tesla	05.09.2017	13.02.2018	15.02.2018	23.02.2018	7,57%
Garmin	06.02.2020	16.07.2020	20.07.2020	28.07.2020	-1,29%
Cognizant	01.11.2019	10.04.2020	14.04.2020	22.04.2020	-2,45%
Boeing	11.10.2017	21.03.2018	23.03.2018	02.04.2018	2,74%
Norsk Hydro	02.10.2018	12.03.2019	14.03.2019	22.03.2019	2,66%
MGM Resorts	04.09.2019	12.02.2020	14.02.2020	24.02.2020	-0,71%
Delta Airlines	19.10.2017	29.03.2018	02.04.2018	10.04.2018	-5,19%
Under Armour	12.10.2017	22.03.2018	26.03.2018	03.04.2018	5,17%
First American	07.12.2018	17.05.2019	21.05.2019	29.05.2019	-3,91%
Quest Diagnostics	17.12.2018	27.05.2019	29.05.2019	06.06.2019	0,07%
Clorox Company	01.03.2023	08.08.2023	11.08.2023	18.08.2023	-4,02%
PepsiCo	05.08.2022	13.01.2023	17.01.2023	25.01.2023	-2,30%
Toyota	14.09.2021	22.02.2022	24.02.2022	04.03.2022	-9,49%
Lockheed Martin	13.12.2010	23.05.2011	25.05.2011	01.06.2011	-3,15%
Walgreens	27.04.2020	05.10.2020	07.10.2020	14.10.2020	-2,22%
Aon	13.09.2021	21.02.2022	23.02.2022	03.03.2022	1,97%
Deutsche Telekom	13.06.2016	21.11.2016	23.11.2016	01.12.2016	0,11%

Zastosowano **test t-Studenta** dla jednej próby:

- **Hipoteza zerowa** H_0:

$$\mu_{CAR} = 0$$

(Cyberataki nie mają wpływu na wartość rynkową, średni CAR wynosi 0).

- **Hipoteza alternatywna** (H_1):

$$\mu_{CAR} < 0$$

(Cyberataki mają negatywny wpływ, średni CAR jest mniejszy od 0).

Obliczona statystyka testowa:

$$t = \frac{\overline{CAR}}{s/\sqrt{n}} = \frac{-0{,}0252}{0{,}0654\sqrt{32}} \approx -2{,}18$$

Na podstawie danych CAR dla 32 firm, średnia skumulowana nadzwyczajna stopa zwrotu wynosi około -0.0251, z odchyleniem standardowym równym 0.0654. Test t daje statystykę t=−2,18 i wartość p≈0.0195

. Ponieważ wartość p jest mniejsza niż 0.05, możemy stwierdzić, że średnia CAR jest statystycznie istotnie mniejsza od zera. Oznacza to, że incydenty cyberbezpieczeństwa miały istotny negatywny wpływ na krótkoterminową wycenę tych firm.

Średni CAR dla całej próby wyniósł:

$$\overline{CAR} = -2.52\%$$

co oznacza, że **średnia wartość rynkowa firm spadła o 2.52%** w krótkim okresie po ujawnieniu cyberataku.

Największe spadki odnotowano dla:

- **SolarWinds** (CAR=−26.1%),

- **Equifax** (CAR=−19,38%).

Niektóre firmy wykazały **pozytywne CAR**, np.:

- **Tesla** (CAR=+7,57 %)
- **Maersk** (CAR=+6,62%)

Pozytywne CAR w przypadku firm Tesla i Maersk mogą wynikać z minimalnego wpływu ataku na operacje (kryptojacking w firmie Tesla nie zakłócił produkcji) lub skutecznego zarządzania kryzysowego (firma Maersk szybko odbudowała systemy po NotPetya)

Analiza wykazała, że **cyberataki mają istotnie negatywny wpływ na krótkoterminową wartość rynkową firm**, co potwierdzają:

- Średni CAR na poziomie **−2,52%**
- Wynik testu **t-Studenta** ($t=-1,98$, $p<0.05$).

Otrzymane wyniki wskazują, że reakcja rynku na cyberataki jest zazwyczaj negatywna, jednak skala spadków wartości rynkowej może zależeć od specyfiki incydentu oraz strategii zarządzania kryzysowego firmy.

6 Wnioski i implikacje

Analiza krótkoterminowego wpływu cyberataków na wartość rynkową firm notowanych na giełdzie, przeprowadzona w ramach niniejszej pracy, dostarczyła szeregu istotnych wniosków, które potwierdzają znaczenie cyberbezpieczeństwa dla stabilności finansowej przedsiębiorstw oraz reakcji rynków finansowych na tego typu incydenty. Analiza, oparta na metodzie *event study*, objęła 32 przypadki cyberataków zarejestrowanych w okresie od 2010 do 2024 roku. Wyniki jednoznacznie wskazują, że ujawnienie cyberataku wywołuje negatywną reakcję rynku, co znajduje odzwierciedlenie w ujemnych wartościach skumulowanych nadzwyczajnych zwrotów (*Cumulative Abnormal Returns*, CAR). Średni CAR dla całej próby wyniósł -2,52%, a statystyczna istotność tego spadku została potwierdzona wynikiem testu t-Studenta ($t=-2,18$, $p<0.05$). W niniejszym rozdziale autor omawia kluczowe wnioski płynące z badania, ich implikacje dla teorii i praktyki zarządzania ryzykiem

cybernetycznym, a także dla polityki regulacyjnej, wskazując jednocześnie ograniczenia badania i potencjalne kierunki dalszych analiz.

Podstawowym wnioskiem płynącym z badania jest *potwierdzenie hipotezy, że cyberataki mają istotnie negatywny wpływ na krótkoterminową wartość rynkową firm notowanych na giełdzie*. Średni CAR na poziomie -2,52% w oknie zdarzenia (-3, +3) wskazuje, że inwestorzy postrzegają informacje o cyberatakach jako sygnał zwiększonego ryzyka, co prowadzi do spadku cen akcji w krótkim okresie po ujawnieniu incydentu. Wynik ten jest spójny z wcześniejszymi badaniami, które również wykazały negatywne reakcje rynku na naruszenia bezpieczeństwa danych[185]. Analiza przeprowadzona w niniejszej pracy koncentrowała się na ogólnym efekcie cyberataków, bez podziału na sektory czy typy incydentów, co pozwoliło na uogólnienie wniosku, że cyberataki stanowią powszechne zagrożenie dla wszystkich firm notowanych na giełdzie, niezależnie od ich specyfiki branżowej. Negatywna reakcja rynku może być interpretowana jako odzwierciedlenie obaw inwestorów dotyczących potencjalnych kosztów związanych z cyberatakami, takich jak straty finansowe, utrata danych, kary regulacyjne czy spadek zaufania klientów. Przykłady firm takich jak firma Equifax czy firma SolarWinds pokazują, że w przypadkach masowych wycieków danych lub ataków na łańcuch dostaw reakcja rynku może być szczególnie silna, co sugeruje, że skala i charakter incydentu mają znaczenie dla percepcji ryzyka. Jednakże średni spadek wartości rynkowej na poziomie -2,52% wskazuje, że nawet w mniej spektakularnych przypadkach cyberataki prowadzą do zauważalnych strat dla akcjonariuszy, co podkreśla powszechność tego zagrożenia w erze cyfrowej.

Mimo ogólnego trendu spadkowego, analiza ujawniła istotne zróżnicowanie w skali reakcji rynku na poszczególne cyberataki. Największe spadki wartości rynkowej zaobserwowano w przypadkach firm, których incydenty miały charakter szczególnie dotkliwy – zarówno pod względem skali naruszenia, jak i potencjalnych konsekwencji dla reputacji i przyszłych przychodów. Na przykład w przypadku firmy SolarWinds atak na łańcuch dostaw, który zainfekował tysiące klientów, wywołał spadek CAR o -26,10%, co odzwierciedla obawy inwestorów o długoterminowe skutki dla pozycji rynkowej firmy. Podobnie, wyciek danych

[185] Arcuri, M., Brogi, M., & Gandolfi, G. (2017). Cyber risk in the financial industry, the market reactions. , 4, 35-49.

firmy Equifax, obejmujący 147 milionów rekordów, skutkował CAR na poziomie -19,38%, co było dodatkowo potęgowane opóźnioną reakcją firmy i utratą wiarygodności.

Z drugiej strony, w niektórych przypadkach odnotowano pozytywne wartości CAR, co stanowi interesujące odstępstwo od ogólnego trendu. Przykładem jest firma Tesla (CAR = +7,52%), gdzie atak typu kryptojacking nie zakłócił kluczowych operacji produkcyjnych, a szybka reakcja firmy mogła zostać odebrana przez inwestorów jako dowód na odporność jej systemów. Podobnie firma Maersk (CAR = +6,62%), mimo poważnego ataku NotPetya, zdołała szybko odbudować infrastrukturę IT i wznowić działalność, co mogło przyczynić się do pozytywnej reakcji rynku. Te przypadki sugerują, że skuteczność zarządzania kryzysowego oraz minimalny wpływ na operacje mogą znacząco modulować reakcję inwestorów, ograniczając straty prowadząc do wzrostu wartości rynkowej. Zróżnicowanie reakcji rynku wskazuje na konieczność uwzględnienia kontekstu incydentu w analizie wpływu cyberataków. Czynniki takie jak rodzaj ataku, jego skala, reakcja firmy oraz jej pozycja rynkowa mogą wpływać na percepcję ryzyka przez inwestorów. Chociaż niniejsze badanie nie analizowało tych zmiennych, wyniki sugerują, że ogólny negatywny wpływ cyberataków nie wyklucza wyjątków, co otwiera pole do dalszych badań nad determinantami reakcji rynkowych.

Wyniki badania mają istotne implikacje dla praktyki zarządzania ryzykiem cybernetycznym w przedsiębiorstwach. Ujemne wartości CAR wskazują, że cyberataki mogą prowadzić do znaczących strat dla akcjonariuszy, co podkreśla potrzebę skutecznych strategii prewencji i reagowania na incydenty. Firmy, które są w stanie szybko i efektywnie odpowiedzieć na cyberatak – poprzez transparentną komunikację, wdrożenie środków zaradczych i inwestycje w bezpieczeństwo – mogą zminimalizować negatywne skutki dla swojej wartości rynkowej, a w niektórych przypadkach osiągnąć pozytywne efekty, jak w przypadku firmy Tesla czy firmy Maersk. Po przeprowadzonej analizie wydaje się, że cyberbezpieczeństwo powinno być integralną częścią strategii zarządzania ryzykiem finansowym. Spadki cen akcji po ujawnieniu incydentu mogą wpływać na koszt kapitału, decyzje inwestycyjne oraz ogólną stabilność finansową przedsiębiorstwa. W związku z tym firmy powinny rozważyć włączenie ryzyka cybernetycznego do swoich modeli wyceny ryzyka, a także opracować strategie hedgingowe, które uwzględniają potencjalne straty wynikające z takich zdarzeń. Inwestycje w zaawansowane technologie ochrony danych, takie jak systemy SIEM (*Security Information and Event Management*) czy EDR (*Endpoint Detection and Response*), mogą okazać się kluczowe dla budowania odporności na cyberataki. Ponadto,

wyniki podkreślają znaczenie komunikacji z interesariuszami po incydencie. Opóźniona lub niejasna reakcja, jak w przypadku firmy Equifax, może pogłębić negatywne skutki rynkowe, podczas gdy szybkie i transparentne działania mogą złagodzić straty. Przedsiębiorstwa powinny zatem opracować plany kryzysowe, które obejmują nie tylko techniczne środki zaradcze, ale także strategie komunikacyjne skierowane do inwestorów, klientów i regulatorów.

W odniesieniu do inwestorów, we wnioskach z badania wskazano na konieczność uwzględniania ryzyka cybernetycznego w procesie podejmowania decyzji inwestycyjnych. Negatywny wpływ cyberataków na wartość rynkową firm sugeruje, że zdolność przedsiębiorstwa do zarządzania tym ryzykiem powinna być jednym z kluczowych kryteriów oceny jego atrakcyjności inwestycyjnej. Firmy, które nie inwestują w odpowiednie zabezpieczenia lub nie dysponują skutecznymi planami reagowania na incydenty, mogą być postrzegane jako bardziej ryzykowne, co może prowadzić do wyższych premii za ryzyko lub niższych wycen ich akcji.

Zróżnicowanie reakcji rynku na poszczególne cyberataki wskazuje również na potencjał wykorzystania informacji o specyfice incydentu i reakcji firmy w strategiach inwestycyjnych. Na przykład szybka i skuteczna odpowiedź na cyberatak może sygnalizować odporność przedsiębiorstwa na atak, co w dłuższym okresie może prowadzić do odbicia cen akcji. Inwestorzy powinni zatem monitorować nie tylko wyniki finansowe spółek, ale także ich politykę cyberbezpieczeństwa i zdolność do zarządzania kryzysowego, aby lepiej ocenić ich stabilność. W kontekście polityki regulacyjnej wyniki badania podkreślają potrzebę wzmacniania wymogów dotyczących cyberbezpieczeństwa. Ujemne CAR po ujawnieniu cyberataków wskazują, że rynek dyscyplinuje firmy za niewystarczające zabezpieczenia, co może stanowić bodziec do zwiększenia inwestycji w ochronę danych. Jednakże, aby zagwarantować minimalny standard bezpieczeństwa, regulatorzy powinni rozważyć wprowadzenie bardziej rygorystycznych przepisów dotyczących raportowania incydentów, audytów bezpieczeństwa oraz minimalnych standardów technologicznych. Analiza sugeruje również, że regulacje powinny być dostosowane do specyfiki różnych sektorów i typów firm. Na przykład przedsiębiorstwa przetwarzające duże liczby danych osobowych, takie jak Equifax czy T-Mobile, mogą wymagać bardziej restrykcyjnych wymogów niż firmy z sektorów mniej narażonych na cyberataki. Wdrożenie takich przepisów mogłoby przyczynić się do zmniejszenia częstotliwości i skali incydentów, a tym samym do ochrony wartości rynkowej firm i stabilności rynków finansowych

Podsumowując, przeprowadzone badanie potwierdziło, że cyberataki mają istotnie negatywny wpływ na krótkoterminową wartość rynkową firm notowanych na giełdzie, co znajduje odzwierciedlenie w średnim CAR na poziomie -2,52%. Wyniki te mogą mieć szerokie implikacje dla teorii finansów i zarządzania ryzykiem, wskazując na potrzebę włączenia polityki cyberbezpieczeństwa do strategii biznesowych i inwestycyjnych. Zróżnicowanie reakcji rynku podkreśla znaczenie skutecznego zarządzania kryzysowego, podczas gdy implikacje regulacyjne wskazują na konieczność dalszego rozwoju polityki w tym zakresie. W obliczu rosnącej liczby i złożoności cyberataków, zrozumienie ich wpływu na rynki finansowe staje się kluczowe dla ochrony wartości przedsiębiorstw i budowania ich odporności na przyszłe zagrożenia.

IV. Sposoby zapewnienia cyberbezpieczeństwa

1. Wpływ cyberbezpieczeństwa na wartość rynkową f rm – potrzeba skutecznych metod ochrony

W dobie cyfryzacji, kiedy dane są uznawane za jeden z najcenniejszych zasobów przedsiębiorstw, cyberbezpieczeństwo stało się kluczowym elementem zarządzania ryzykiem strategicznym. Cyberataki, takie jak wycieki danych, ataki *ransomware* czy incydenty DDoS, nie tylko zagrażają integralności systemów informatycznych, ale także wywierają istotny wpływ na stabilność finansową i reputację firm. W kontekście rynków finansowych, gdzie zaufanie inwestorów i kapitalizacja rynkowa odgrywają decydującą rolę, brak skutecznych metod ochrony przed cyberzagrożeniami może prowadzić do dramatycznych spadków wartości rynkowej, utraty konkurencyjności i długoterminowych strat. W niniejszym podrozdziale autor szczegółowo omówi wpływ cyberbezpieczeństwa na wartość rynkową przedsiębiorstw, przeanalizuje mechanizmy tego oddziaływania oraz wykaże, że inwestycje w nowoczesne technologie i strategie ochrony danych są nie tylko koniecznością, ale także strategiczną przewagą w ochronie stabilności rynkowej.

Konkretnym przykładem jest atak na Equifax w 2017 roku, jedną z największych agencji kredytowych w USA. W wyniku wycieku danych osobowych 147 milionów klientów, w tym numerów kart kredytowych i danych identyfikacyjnych, ogłoszonego 7 września 2017 roku, kapitalizacja rynkowa firmy spadła o ponad 4 miliardy dolarów w ciągu tygodnia. Akcje Equifax straciły 13,7% wartości w dniu ujawnienia. Ten drastyczny spadek był wynikiem nie tylko bezpośrednich kosztów incydentu, ale także utraty zaufania inwestorów do zdolności zarządu do skutecznego zarządzania ryzykiem cybernetycznym. Innym znamiennym przykładem jest atak na sieć Target w 2013 roku. Hakerzy skradli dane 40 milionów kart płatniczych klientów, co ogłoszono w grudniu tego roku. Należy zauażyć, że w ciągu miesiąca akcje firmy spadły o 11%, a koszty związane z incydentem – w tym odszkodowania, modernizacja systemów i kary regulacyjne – wyniosły 252 miliony dolarów. Co więcej, Target zanotował spadek przychodów w okresie świątecznym, co dodatkowo pogłębiło straty. Ten przypadek ilustruje, jak cyberataki mogą wpływać nie tylko na wycenę rynkową, ale także na bieżące wyniki finansowe i relacje z klientami.

Negatywne skutki cyberataków na wartość rynkową wynikają z szeregu powiązanych mechanizmów, które oddziałują na percepcję ryzyka przez inwestorów i innych interesariuszy. Jednym z mechanizmów jest utrata zaufania do zdolności firmy do zarządzania ryzykiem operacyjnym. Cyberatak jest często interpretowany jako dowód słabości infrastruktury IT i procesów zarządzania, co budzi obawy o przyszłe incydenty i ich potencjalne konsekwencje. Inwestorzy, przewidując koszty związane z naprawą systemów, odszkodowaniami i karami regulacyjnymi, mogą obniżać wycenę akcji, co prowadzi do natychmiastowych spadków kapitalizacji rynkowej.

Kolejnym kluczowym mechanizmem są koszty prawne i regulacyjne. Firmy, które nie przestrzegają wymogów ochrony danych, takich jak RODO[186] w Europie czy CCPA[187] w Stanach Zjednoczonych, narażają się na wysokie kary finansowe. Przykładowo, firma Equifax, w ramach ugody z Federalną Komisją Handlu (FTC) w 2019 roku, zapłaciła 700 milionów dolarów za naruszenie przepisów. Dodatkowo, pozwy zbiorowe od poszkodowanych klientów, jak w przypadku firmy Target, gdzie koszty prawne sięgnęły dziesiątek milionów dolarów, zwiększają obciążenia finansowe i negatywnie wpływają na postrzeganie firmy na rynku[188].

Warto również rozważyć długoterminowe skutki dla konkurencyjności organizacji. Firmy, które nie inwestują w cyberbezpieczeństwo, mogą utracić przewagę na rzecz konkurentów z bardziej skutecznymi systemami ochrony. Na przykład, po ataku na firmę Sony Pictures w 2014 roku, gdzie skradziono poufne dane filmowe i e-maile, firma musiała zmierzyć się nie tylko z kosztami finansowymi (szacowanymi na 100 milionów dolarów), ale także z utratą pozycji na rynku rozrywki. W dobie rosnącej świadomości konsumentów i inwestorów, przedsiębiorstwa z zaawansowaną polityką cyberbezpieczeństwa są postrzegane jako bardziej stabilne i wiarygodne, co zwiększa ich atrakcyjność inwestycyjną.

W obliczu rosnących zagrożeń cybernetycznych inwestycje w cyberbezpieczeństwo przestają być postrzegane jako koszt operacyjny, a stają się elementem strategicznym dla

---

[186] Parlament Europejski i Rada Unii Europejskiej, *Rozporządzenie (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO)*, Dz.U. UE L 119 z 4.5.2016, s. 1–88.

[187] California State Legislature, *California Consumer Privacy Act of 2018 (CCPA)*, California Civil Code §§ 1798.100–1798.199, Sacramento 2018 (z późn. zm. *California Privacy Rights Act of 2020 – CPRA*)

[188] Kamiya, S., Kang, J., Kim, J., Milidonis, A., & Stulz, R. (2018). What is the Impact of Successful Cyberattacks on Target Firms?. *S&P Global Market Intelligence Research Paper Series*. https://doi.org/10.2139/ssrn.3135514.

ochrony wartości rynkowej. Nowoczesne technologie, takie jak zapory sieciowe (firewalls), systemy wykrywania i zapobiegania intruzom (IDS/IPS), szyfrowanie danych czy sztuczna inteligencja w analizie zagrożeń, pozwalają firmom minimalizować ryzyko incydentów i budować zaufanie interesariuszy. Wdrożenie takich rozwiązań nie tylko chroni przed stratami finansowymi i reputacyjnymi, ale także wzmacnia wizerunek firmy jako odpowiedzialnego podmiotu rynkowego. Przykładem skutecznego zarządzania kryzysem jest reakcja firmy Maersk na atak *ransomware* NotPetya w 2017 roku. Atak sparaliżował systemy IT firmy i zakłócił operacje w 76 portach na świecie, powodując początkowy spadek akcji o 2%. Jednak dzięki szybkiemu przywróceniu infrastruktury i transparentnej komunikacji z inwestorami, Maersk osiągnął pozytywny CAR na poziomie +3,93% w oknie zdarzenia. Ten przypadek pokazuje, że skuteczna strategia cyberbezpieczeństwa może nie tylko ograniczyć straty, ale także przyspieszyć powrót do stabilności rynkowej[189]. Dodatkowo, cyberbezpieczeństwo może być czynnikiem różnicującym na tle konkurencji. Firmy takie jak Microsoft, które regularnie inwestują w badania i rozwój w dziedzinie ochrony danych (np. Azure Security Center), nie tylko minimalizują ryzyko, ale także budują markę lidera w zakresie innowacji technologicznych. W efekcie, ich wartość rynkowa pozostaje stabilna, a inwestorzy postrzegają je jako mniej narażone na skutki cyberataków w porównaniu z konkurentami o słabszych zabezpieczeniach[190].

Rosnąca liczba cyberataków zwiększa presję na wprowadzanie regulacji dotyczących ochrony danych, co dodatkowo podkreśla znaczenie cyberbezpieczeństwa dla wartości rynkowej. Wprowadzenie RODO (GDPR) w Unii Europejskiej w 2018 roku nałożyło na firmy obowiązek zapewnienia odpowiednich zabezpieczeń pod groźbą kar sięgających 20 milionów euro lub 4% rocznego obrotu. Na przykład, firma British Airways otrzymała karę 20 milionów funtów w 2020 roku za wyciek danych 400 tysięcy klientów, co dodatkowo obciążyło finanse firmy i wpłynęło na jej wycenę rynkową[191]. Równolegle rośnie świadomość społeczna na temat cyberzagrożeń, co wpływa na decyzje konsumenckie i inwestycyjne. Klienci coraz częściej

[189] Havakhor, T., Rahman, M., & Zhang, T. (2021). Disclosure of Cybersecurity Investments and the Cost of Capital. *ERN: Technology (Topic)*. https://doi.org/10.2139/ssrn.3553470.
[190] Microsoft. (2021). *Microsoft Digital Defense Report 2021*. Pobrano z https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2021
[191] Ford, A., Al-Nemrat, A., Ghorashi, S., & Davidson, J. (2022). The impact of GDPR infringement fines on the market value of firms. *Inf. Comput. Secur.*, 31, 51-64. https://doi.org/10.1108/ics-03-2022-0049.

wybierają firmy, które gwarantują bezpieczeństwo danych, co zmusza przedsiębiorstwa do priorytetowego traktowania tego obszaru[192].

2. Profilaktyka cybernetyczna jako strategia minimalizacji strat finansowych

W obliczu rosnącej liczby i złożoności cyberataków, należy zauważyć że profilaktyka cybernetyczna staje się kluczowym elementem strategii zarządzania ryzykiem w przedsiębiorstwach. Dlatego podejście oparte na zapobieganiu incydentom, zanim one wystąpią, jest nie tylko bardziej efektywne, ale również znacznie mniej kosztowne niż reagowanie na skutki naruszeń bezpieczeństwa. W niniejszym podrozdziale autor omówi rolę profilaktyki cybernetycznej w minimalizacji strat finansowych. Analizie poddane zostaną technologie prewencyjne, takie jak zapory sieciowe, szyfrowanie danych oraz systemy wczesnego ostrzegania, a także znaczenie szkoleń pracowników jako ekonomicznej formy prewencji. Na zakończenie przedstawiona zostanie analiza porównawcza kosztów wdrożenia profilaktyki z kosztami reakcji na incydenty, wskazując na wymierne korzyści płynące z inwestycji w zapobieganie zagrożeniom.

Technologie prewencyjne pełnią funkcję pierwszej linii obrony przed cyberzagrożeniami, mając na celu utrudnienie lub uniemożliwienie realizacji ataku. Do kluczowych rozwiązań w tej kategorii należą zaliczyć zapory sieciowe, systemy szyfrowania danych oraz systemy wczesnego ostrzegania, takie jak systemy wykrywania intruzów (Intrusion Detection Systems, IDS). Ich działanie opiera się na filtrowaniu ruchu sieciowego, zabezpieczaniu poufności informacji oraz identyfikacji potencjalnych zagrożeń na wczesnym etapie. Zapory sieciowe kontrolują ruch sieciowy na podstawie wcześniej zdefiniowanych reguł, blokując nieautoryzowany dostęp i chroniąc przed znanymi typami ataków. Współczesne zapory nowej generacji (next-generation firewalls, NGFW) wprowadzają zaawansowane funkcjonalności, takie jak głęboka inspekcja pakietów (deep packet inspection, DPI). Dzięki analizie zawartości przesyłanych danych, a nie tylko ich nagłówków, NGFW są w stanie wykrywać i neutralizować bardziej złożone zagrożenia, na przykład ataki wykorzystujące luki

[192] Yang, L., Lau, L. K., & Gan, H. (2020). *Investors' perceptions of the cybersecurity risk management reporting framework*. *International Journal of Accounting and Information Management, 28*, 167-183.

w aplikacjach. Ich wdrożenie pozwala organizacjom na znaczące podniesienie poziomu bezpieczeństwa infrastruktury sieciowej[193].

Kolejnym filarem technologii prewencyjnych jest szyfrowanie danych, które zabezpiecza poufność i integralność informacji. Algorytmy takie jak AES (Advanced Encryption Standard) czy RSA (Rivest-Shamir-Adleman) znajdują szerokie zastosowanie w ochronie danych zarówno w spoczynku, jak i w trakcie transmisji[194]. Wraz z rozwojem chmur obliczeniowych coraz większe znaczenie zyskują techniki takie jak szyfrowanie homomorficzne (homomorphic encryption), które umożliwiają przetwarzanie danych bez konieczności ich deszyfrowania. Rozwiązanie to pozwala na zachowanie wysokiego poziomu bezpieczeństwa w środowiskach rozproszonych, co jest szczególnie istotne w kontekście współczesnych modeli biznesowych opartych na outsourcingu i zdalnym dostępie[195]. Natomiast systemy wczesnego ostrzegania, takie jak IDS, odgrywają istotną rolę w monitorowaniu sieci i systemów w celu identyfikacji podejrzanej aktywności. Mogą one funkcjonować w trybie pasywnym, generując ostrzeżenia dla administratorów, lub w trybie aktywnym jako systemy zapobiegania intruzom (Intrusion Prevention Systems, IPS), które automatycznie blokują wykryte zagrożenia. Ich efektywność wzrasta dzięki integracji z algorytmami uczenia maszynowego, które umożliwiają rozpoznawanie nietypowych wzorców zachowań, wskazujących na nieznane dotychczas ataki. Tego typu rozwiązania stają się nieodzownym elementem strategii prewencyjnych w organizacjach narażonych na dynamicznie ewoluujące zagrożenia cybernetyczne[196].

Pomimo zaawansowania technologicznych środków ochrony, czynnik ludzki pozostaje jednym z najbardziej narażonych elementów w systemie cyberbezpieczeństwa. Ataki socjotechniczne, takie jak phishing, często wykorzystują błędy pracowników do uzyskania nieautoryzowanego dostępu do infrastruktury organizacji. W tym kontekście szkolenia personelu w zakresie zasad higieny cybernetycznej jawią się jako najtańsza, a zarazem wysoce

[193] Lei, S. (2024). Synergizing next-generation firewalls and defense-in-depth strategies in a dynamic cybersecurity landscape. , 13175, 131750M - 131750M-7. https://doi.org/10.1117/12.3031957.

[194] National Institute of Standards and Technology (NIST), *Advanced Encryption Standard (AES) – FIPS Publication 197*, Gaithersburg, MD 2001. (nvlpubs.nist.gov – dostęp: 24.03 2025).
[195] Lv, Y. (2021). Data privacy protection based on homomorphic encryption. *Journal of Physics: Conference Series*, 2037. https://doi.org/10.1088/1742-6596/2037/1/012129.
[196] Kathiresan, V., Karthik, S., Divya, P., & Rajan, D. (2022). A Comparative Study of Diverse Intrusion Detection Methods using Machine Learning Techniques. *2022 International Conference on Computer Communication and Informatics (ICCCI)*, 1-6. https://doi.org/10.1109/ICCCI54379.2022.9740744.

skuteczna forma profilaktyki. Programy edukacyjne koncentrują się na rozwijaniu umiejętności rozpoznawania podejrzanych wiadomości, stosowania bezpiecznych haseł oraz unikania ryzykownych działań w środowisku cyfrowym. Badania empiryczne wskazują, że systematyczne szkolenia mogą zredukować ryzyko skutecznych ataków phishingowych o 70-90%. Szkolenia wykraczają poza samą prewencję techniczną, budując w organizacji kulturę bezpieczeństwa. Pracownicy, którzy zdają sobie sprawę z konsekwencji cyberzagrożeń, są bardziej skłonni do przestrzegania procedur oraz zgłaszania potencjalnych incydentów, co znacząco obniża ryzyko naruszeń. W dłuższej perspektywie takie podejście przekłada się na zwiększoną odporność organizacji na ataki, wzmacniając jej zdolność do funkcjonowania w środowisku o wysokim poziomie zagrożenia cyfrowego[197].

Inwestycje w profilaktykę cybernetyczną, choć wiążą się z koniecznością poniesienia początkowych nakładów, okazują się znacznie bardziej opłacalne niż koszty wynikające z reagowania na zaistniałe incydenty. Z raportu IBM za 2024 rok wynika, że średni koszt naruszenia danych w Stanach Zjednoczonych wyniósł 4,88 miliona dolarów, przy czym znaczną część tej kwoty stanowiły wydatki na wykrycie i deskalację problemu (1,5 miliona dolarów) oraz straty biznesowe (1,2 miliona dolarów). Wdrożenie rozwiązań prewencyjnych, takich jak zapory sieciowe, systemy IDS czy programy szkoleniowe, może zredukować te koszty o 30-50%, oferując wymierne oszczędności[198].

W perspektywie długoterminowej profilaktyka cybernetyczna przynosi korzyści wykraczające poza bezpośrednie oszczędności finansowe. Chroniąc reputację organizacji i jej wartość rynkową, wspiera ona stabilność biznesową i konkurencyjność na rynku. W dobie coraz bardziej wyrafinowanych cyberataków, podejście oparte na prewencji staje się nie tylko racjonalnym wyborem ekonomicznym, ale także strategicznym imperatywem dla przedsiębiorstw działających w środowisku globalnym.

[197] Khan, M., & Muntaha, S. (2024). Evaluating the effectiveness of cybersecurity awareness programs in reducing phishing attacks: A qualitative study. *World Journal of Advanced Research and Reviews*. https://doi.org/10.30574/wjarr.2024.23.2.2538.
[198] IBM. (2024). *Cost of a Data Breach Report 2043*. Pobrano z https://www.ibm.com/reports/data-breach

3. Reagowanie na incydenty – ograniczanie wpływu na rynki f nansowe

W erze cyfryzacji, gdzie cyberataki stają się jednym z najpoważniejszych zagrożeń dla przedsiębiorstw, zdolność do skutecznego reagowania na incydenty cybernetyczne jest kluczowym elementem ochrony nie tylko danych i infrastruktury, ale również wartości rynkowej oraz zaufania inwestorów. Ataki takie jak wycieki danych, *ransomware* czy naruszenia integralności systemów mogą prowadzić do natychmiastowych spadków cen akcji, utraty reputacji i długoterminowych strat finansowych. W tym kontekście procedury zarządzania kryzysowego, wsparte nowoczesnymi technologiami, takimi jak systemy zapobiegania intruzom (IPS) oraz systemy zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM), odgrywają fundamentalną rolę w minimalizowaniu wpływu tych incydentów na rynki finansowe. W niniejszym podrozdziale autor dokona analizy metod reagowania na cyberataki, które pozwalają przedsiębiorstwom ograniczyć ich negatywne skutki dla wartości rynkowej i zaufania inwestorów. Omówione zostaną procedury zarządzania kryzysowego, w tym szybkie powiadamianie interesariuszy i odzyskiwanie danych, rola systemów IPS i SIEM w natychmiastowej reakcji na zagrożenia, a także konkretne studia przypadków, takie jak skuteczna reakcja firmy Anthem po ataku w 2015 roku, które pokazują, jak dobrze zaplanowane działania mogą zmniejszyć straty finansowe[199].

Zarządzanie kryzysowe w przypadku cyberataków opiera się na zestawie precyzyjnie określonych procedur, których celem jest szybkie zidentyfikowanie incydentu, ograniczenie jego skutków oraz przywrócenie normalnego funkcjonowania przedsiębiorstwa. Kluczowym elementem jest tutaj opracowanie i wdrożenie planu reagowania na incydenty, który definiuje role i obowiązki zespołu ds. bezpieczeństwa, procedury eskalacji oraz kanały komunikacji. Taki plan pozwala na skoordynowane działanie w sytuacji kryzysowej, minimalizując chaos i skracając czas reakcji, co jest szczególnie istotne dla firm notowanych na giełdzie, gdzie każda chwila przestoju może wiązać się z poważnymi stratami finansowymi. Szybkie powiadamianie interesariuszy – klientów, partnerów biznesowych, regulatorów i inwestorów – jest jednym z najważniejszych aspektów tego procesu. Badania wskazują, że transparentność i szybkość w informowaniu o incydencie mogą znacząco wpłynąć na percepcję rynku i utrzymanie zaufania

[199] Perols, R. (2023). The Impact of the Type of Cybersecurity Assurance Service and Cybersecurity Incidents on Investor Perceptions and Decisions. *Auditing: A Journal of Practice & Theory*. https://doi.org/10.2308/ajpt-19-022.

do przedsiębiorstwa.[200]. Opóźnienie w powiadomieniu interesariuszy pogłębiło kryzys zaufania, co miało bezpośrednie przełożenie na wartość rynkową firmy. Z kolei firma Adobe, która w 2013 roku padła ofiarą ataku, w wyniku którego skradziono dane 38 milionów użytkowników, podjęła natychmiastowe działania, informując klientów o incydencie i oferując im bezpłatne monitorowanie kredytowe. Dzięki transparentnej komunikacji i szybkiemu reagowaniu spadek akcji Adobe wyniósł zaledwie 2% w ciągu miesiąca, co pokazuje, jak skuteczne podejście może ograniczyć negatywne skutki dla wartości rynkowej[201].

Odzyskiwanie danych, określane również jako *disaster recovery*, stanowi kolejny kluczowy filar zarządzania kryzysowego. Posiadanie aktualnych kopii zapasowych oraz dobrze przygotowanych planów przywracania systemów pozwala na szybkie wznowienie operacji biznesowych po ataku. Przykładem skutecznego zastosowania takich procedur jest przypadek firmy Maersk, która w 2017 roku została zaatakowana przez ransomware NotPetya. Atak ten sparaliżował systemy informatyczne firmy i zakłócił działalność w 76 portach na całym świecie. Dzięki efektywnemu planowi odzyskiwania danych firma Maersk zdołała przywrócić swoje systemy w ciągu 10 dni, co pozwoliło ograniczyć straty do 300 milionów dolarów – wyniku znacznie lepszego niż początkowe prognozy. Szybkie przywrócenie działalności nie tylko zminimalizowało straty operacyjne, ale także wzmocniło zaufanie inwestorów, sygnalizując gotowość firmy na sytuacje kryzysowe. Te przykłady pokazują, że skuteczne procedury zarządzania kryzysowego, obejmujące zarówno szybkie powiadamianie interesariuszy, jak i odzyskiwanie danych, są nieodzowne dla minimalizowania wpływu cyberataków na rynki finansowe. Firmy, które inwestują w takie rozwiązania, mogą nie tylko ograniczyć bezpośrednie straty, ale także chronić swoją reputację i wartość rynkową w oczach inwestorów[202].

Równie istotną rolę w reagowaniu na cyberataki odgrywają nowoczesne technologie, takie jak systemy zapobiegania intruzom (IPS) oraz systemy zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM). Systemy IPS monitorują ruch sieciowy w czasie rzeczywistym, analizując go pod kątem podejrzanych wzorców i blokując potencjalnie

[200] Thompson, E. (2018). The Significance of Incident Response. , 1-10. https://doi.org/10.1007/978-1-4842-3870-7_1.
[201] Kelton, A., & Pennington, R. (2020). Do Voluntary Disclosures Mitigate the Cybersecurity Breach Contagion Effect?. *J. Inf. Syst.*, 34, 133-157. https://doi.org/10.2308/isys-52628.
[202] Gudimetla, S. (2024). Cybersecurity Considerations in Disaster Recovery Planning. *International Journal for Research in Applied Science and Engineering Technology*. https://doi.org/10.22214/ijraset.2024.62253.

niebezpieczne działania, zanim te zdążą wyrządzić szkody. Wykorzystują one techniki takie jak analiza sygnatur, która porównuje ruch sieciowy z bazą znanych wzorców ataków oraz analiza anomalii, która identyfikuje odstępstwa od normalnego zachowania systemów. Dzięki temu są w stanie wykrywać zarówno znane, jak i nieznane zagrożenia, co jest kluczowe w obliczu rosnącej liczby ataków typu *zero-day*. Z kolei systemy SIEM agregują dane z różnych źródeł – takich jak logi systemowe, alerty IDS czy dane telemetryczne – tworząc kompleksowy obraz sytuacji bezpieczeństwa przedsiębiorstwa. Dzięki analizie korelacyjnej mogą one zidentyfikować wzorce wskazujące na potencjalne incydenty, na przykład próby ataku *brute-force* poprzez wykrycie nadmiernej liczby nieudanych logowań z jednego adresu IP. Integracja SIEM z narzędziami automatyzacji, takimi jak SOAR, umożliwia dodatkowo automatyczne uruchamianie procedur naprawczych, takich jak blokowanie podejrzanych adresów IP czy izolacja zainfekowanych hostów. W praktyce systemy te pozwalają na szybkie zlokalizowanie źródła ataku i ograniczenie jego rozprzestrzeniania się[203]. Przykładem może być atak na firmę SolarWinds w 2020 roku, w której zaawansowane złośliwe oprogramowanie Sunburst zainfekowało tysiące organizacji poprzez łańcuch dostaw. Firmy korzystające z systemów SIEM były w stanie szybko zidentyfikować podejrzaną aktywność, taką jak nieautoryzowane połączenia z serwerami kontroli i podjąć działania zaradcze, co znacząco ograniczyło szkody operacyjne i finansowe[204]. Co więcej, integracja tych systemów z technologiami uczenia maszynowego (ML) jeszcze bardziej zwiększa ich skuteczność. Algorytmy ML analizują ogromne liczby danych w czasie rzeczywistym, wykrywając subtelne wzorce zachowań, które mogą wskazywać na ataki – na przykład nagły wzrost transferu danych do nieznanych lokalizacji, co może sugerować eksfiltrację danych. Dzięki temu systemy IPS i SIEM stają się nieodzownymi narzędziami w natychmiastowej reakcji na zagrożenia, pomagając firmom minimalizować wpływ cyberataków na ich stabilność finansową[205].

Analiza konkretnych przypadków pozwala lepiej zrozumieć, jak skuteczne reagowanie na incydenty może ograniczyć straty finansowe i chronić wartość rynkową przedsiębiorstwa.

[203] Sheeraz, M., Durad, M., Tahir, S., Tahir, H., Saeed, S., & Almuhaideb, A. (2024). Advancing Snort IPS to Achieve Line Rate Traffic Processing for Effective Network Security Monitoring. *IEEE Access*, 12, 61848-61859. https://doi.org/10.1109/ACCESS.2024.3395123.

[204] Kruti, A., Butt, U., & Sulaiman, R. (2023). A review of SolarWinds attack on Orion platform using persistent threat agents and techniques for gaining unauthorized access. .

[205] Nurusheva, A., Medelbayeva, N., Satybaldina, D., & Goranin, N. (2024). Machine learning algorithms in SIEM systems for enhanced detection and management of security events. *Bulletin of L.N. Gumilyov Eurasian National University. Mathematics, computer science, mechanics series*. https://doi.org/10.32523/bulmathenu.2024/3.1.

W lutym 2015 r. spółka Anthem Inc., jeden z największych ubezpieczycieli zdrowotnych w USA, ogłosiła kradzież danych osobowych 78,8 mln klientów w wyniku kampanii phishingowej. Choć incydent nie obejmował historii medycznych ani danych kart płatniczych, jego skala ujawniła słabości w obszarze szyfrowania danych „w spoczynku". Spółka zareagowała natychmiast: uruchomiła specjalny portal dla klientów, zaoferowała darmowe monitorowanie kredytowe, powołała niezależnych ekspertów ds. cyberbezpieczeństwa oraz zgłosiła incydent do organów federalnych i stanowych. Reakcja była oceniana jako relatywnie szybka i profesjonalna, co pozwoliło ograniczyć straty reputacyjne oraz krótkoterminowy spadek kursu akcji (CAR = –4,19%). Przypadek Anthem jest dziś wskazywany w literaturze branżowej jako przykład dobrze zaplanowanego planu IR oraz impulsu do modernizacji procedur bezpieczeństwa w całym sektorze ochrony zdrowia.[206]. Z kolei atak na firmę Marriott International w 2018 roku, w której wyciekły dane 500 milionów gości hotelowych pokazuje, jak brak szybkiej i skutecznej reakcji może pogłębić straty. Firma wykryła incydent z opóźnieniem, a jej odpowiedzi były powolne i niejasne, co doprowadziło do spadku akcji o 5,6% w dniu ujawnienia ataku oraz nałożenia grzywny w wysokości 18,4 miliona funtów przez brytyjski organ regulacyjny ICO. Opóźniona komunikacja i brak efektywnego zarządzania kryzysowego zwiększyły straty finansowe i reputacyjne[207] . Te przypadki jasno wskazują, że skuteczność reakcji na cyberatak ma bezpośredni wpływ na zdolność firmy do ochrony swojej wartości rynkowej i zaufania inwestorów.

Reagowanie na incydenty cybernetyczne jest zatem kluczowym elementem ochrony stabilności finansowej przedsiębiorstw w obliczu rosnącego zagrożenia cyberatakami. Procedury zarządzania kryzysowego, takie jak szybkie powiadamianie interesariuszy i odzyskiwanie danych, w połączeniu z zaawansowanymi technologiami, takimi jak systemy IPS i SIEM, pozwalają na skuteczne ograniczenie negatywnych skutków incydentów dla wartości rynkowej i zaufania inwestorów. Przedstawione studia przypadku, pokazują, że dobrze zaplanowane i szybko wdrożone działania mogą znacząco zmniejszyć straty finansowe, podczas gdy opóźnienia i brak transparentności, jak w przypadku firmy Marriott, mogą prowadzić do eskalacji kryzysu. W dobie coraz bardziej wyrafinowanych cyberzagrożeń inwestycje w strategie reagowania na incydenty stają się nieodzowne dla utrzymania stabilności

[206] Sullivan, C. (2016). The 2014 Sony Hack and the Role of International Law. , 8, 1.
[207] Aivazpour, Z., Valecha, R., & Chakraborty, R. (2022). Data Breaches. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 53, 65 - 82. https://doi.org/10.1145/3571823.3571829.

na rynkach finansowych. Firmy, które są w stanie szybko i efektywnie reagować na ataki, nie tylko minimalizują bezpośrednie straty, ale także budują odporność na przyszłe incydenty, co w dłuższej perspektywie przekłada się na ich konkurencyjność i zdolność do ochrony interesów swoich interesariuszy. Wraz z rozwojem technologii i ewolucją zagrożeń cybernetycznych, dalsze doskonalenie tych metod będzie kluczowe dla zapewnienia bezpieczeństwa i stabilności rynków finansowych w przyszłości.

4. Budowanie odporności rynkowej przez cyberbezpieczeństwo

W erze cyfryzacji, w której przedsiębiorstwa stają się coraz bardziej zależne od technologii informatycznych, cyberbezpieczeństwo przestało być jedynie technicznym zagadnieniem ochrony danych i systemów. Stało się strategicznym narzędziem, które pozwala firmom budować odporność rynkową, zwiększać stabilność finansową i wzmacniać swoją pozycję konkurencyjną. Celem niniejszego rozdziału jest gruntowna analiza tego, jak długoterminowe strategie cyberbezpieczeństwa mogą wpływać na wartość rynkową przedsiębiorstw, uwzględniając zarówno aspekty regulacyjne, technologiczne, jak i organizacyjne. W szczególności omówione zostaną:

- rola regulacji prawnych w zapewnieniu stabilności firm,
- znaczenie współpracy międzysektorowej w przeciwdziałaniu cyberzagrożeniom,
- inwestycje w nowoczesne technologie takie jak sztuczna inteligencja i uczenie maszynowe, a także
- budowanie kultury bezpieczeństwa w organizacji.

Każdy z tych elementów zostanie poparty przykładami z praktyki biznesowej oraz wynikami badań naukowych, aby wykazać, że cyberbezpieczeństwo jest nie tylko kosztem, ale przede wszystkim inwestycją w przyszłość przedsiębiorstwa na konkurencyjnym rynku globalnym.

Regulacje prawne pełnią kluczową rolę w kształtowaniu podejścia przedsiębiorstw do cyberbezpieczeństwa, wymuszając wdrożenie zaawansowanych systemów ochrony danych i infrastruktury krytycznej. W Unii Europejskiej Rozporządzenie o Ochronie Danych (RODO), wprowadzone w maju 2018 roku, ustanowiło nowe standardy w zakresie ochrony danych osobowych, nakładając na firmy obowiązek stosowania takich środków jak szyfrowanie, regularne audyty bezpieczeństwa czy procedury reagowania na naruszenia danych.

Nieprzestrzeganie tych wymogów może skutkować karami finansowymi sięgającymi 20 milionów euro lub 4% rocznego obrotu firmy – co w przypadku dużych korporacji oznacza potencjalne straty rzędu setek milionów euro. Na przykład w 2019 roku francuski organ ochrony danych (CNIL) nałożył na firmę Google karę w wysokości 50 milionów euro za brak odpowiedniej transparentności w przetwarzaniu danych, co było wyraźnym sygnałem dla innych firm o konieczności dostosowania się do regulacji[208].

Podobne znaczenie ma dyrektywa NIS2 (*Network and Information Security Directive*)[209], która weszła w życie w 2023 roku jako odpowiedź na rosnące zagrożenia cybernetyczne w sektorze usług kluczowych, takich jak finanse, energetyka czy transport. Dyrektywa ta nakłada na przedsiębiorstwa obowiązek wdrażania systemów wczesnego ostrzegania, raportowania incydentów oraz współpracy z krajowymi organami ds. cyberbezpieczeństwa. W sektorze finansowym szczególne znaczenie ma również DORA (*Digital Operational Resilience Act*)[210], który od 2025 roku będzie regulował odporność cyfrową instytucji finansowych w Unii Europejskiej, wymagając od banków, ubezpieczycieli i innych podmiotów regularnego testowania swoich systemów na wypadek cyberataków. Choć wdrożenie tych regulacji wiąże się z istotnymi kosztami – szacowanymi na przykład przez Europejską Agencję Cyberbezpieczeństwa (ENISA) na średnio 1-2% rocznego budżetu IT przedsiębiorstw – przynosi ono również korzyści w postaci zwiększonej odporności na zagrożenia cyfrowe[211].

Realizacja działań zgodnie z prawem pozwala również unikać kosztów związanych z karami i utratą reputacji. Przykładem może być brytyjska firma British Airways, która w 2018 roku doświadczyła wycieku danych 380 000 klientów, co skutkowało karą w wysokości 20 milionów funtów nałożoną przez brytyjski urząd ds. ochrony danych (ICO) w 2020 roku. W

[208] Ford, A., Al-Nemrat, A., Ghorashi, S., & Davidson, J. (2022). The impact of GDPR infringement fines on the market value of firms. *Inf. Comput. Secur.*, 31, 51-64. https://doi.org/10.1108/ics-03-2022-0049.

[209] Parlament Europejski i Rada Unii Europejskiej, *Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (NIS2)*, Dz.U. UE L 333 z 27.12.2022, s. 80–152.

[210] Parlament Europejski i Rada Unii Europejskiej, *Rozporządzenie (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie cyfrowej odporności operacyjnej sektora finansowego (DORA)*, Dz.U. UE L 333 z 27.12.2022, s. 1–102.

[211] Carrapico, H., & Farrand, B. (2024). Cybersecurity Trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics. *JCMS: Journal of Common Market Studies*. https://doi.org/10.1111/jcms.13654.

dłuższej perspektywie firmy, które traktują regulacje prawne jako integralną część swojej strategii cyberbezpieczeństwa, zyskują przewagę konkurencyjną, minimalizując ryzyko nagłych spadków wartości rynkowej spowodowanych cyberincydentami. Inwestorzy, zwłaszcza ci nastawieni na długoterminowe zyski, doceniają przewidywalność i stabilność, a zgodność z przepisami staje się jednym z kluczowych wskaźników gotowości firmy na wyzwania ery cyfrowej[212].

W obliczu coraz bardziej wyrafinowanych i globalnych cyberataków pojedyncze przedsiębiorstwo nie jest w stanie samodzielnie stawić czoła wszystkim zagrożeniom. Współpraca międzysektorowa, polegająca na dzieleniu się informacjami o zagrożeniach, staje się niezbędnym elementem budowania odporności rynkowej. Organizacje takie jak ISAC (*Information Sharing and Analysis Centers*) odgrywają kluczową rolę w tym procesie, umożliwiając firmom wymianę danych o nowych lukach w zabezpieczeniach, technikach ataków i skutecznych strategiach obronnych. W sektorze finansowym szczególnie aktywną rolę pełni FS-ISAC (*Financial Services Information Sharing and Analysis Center*), które zrzesza banki, instytucje płatnicze, giełdy i inne podmioty w celu wspólnego monitorowania i reagowania na cyberzagrożenia. W 2020 roku FS-ISAC odegrało kluczową rolę w ograniczeniu skutków masowych ataków DDoS na systemy płatnicze w Europie i Ameryce Północnej. Dzięki wymianie informacji w czasie rzeczywistym banki mogły szybko wdrożyć odpowiednie zabezpieczenia, co zapobiegło poważnym zakłóceniom w funkcjonowaniu rynku finansowego[213]. Efektywność współpracy międzysektorowej potwierdzają także inne przykłady. W 2021 roku organizacja H-ISAC (*Health Information Sharing and Analysis Center*) pomogła szpitalom w Ameryce Północnej zminimalizować skutki ataków *ransomware*, które nasiliły się w czasie pandemii COVID-19. Dzięki wspólnemu dzieleniu się informacjami o taktykach hakerów szpitale mogły szybciej aktualizować swoje systemy zabezpieczeń, co uchroniło je przed paraliżem operacyjnym i potencjalnymi stratami finansowymi sięgającymi milionów dolarów[214]. Współpraca ta nie tylko zwiększa odporność poszczególnych firm, ale także wzmacnia stabilność całego sektora, minimalizując ryzyko systemowe, które mogłoby

[212] Enoma, B. (2020). Data breach in the travel sector and strategies for risk mitigation. *Journal of Data Protection & Privacy*. https://doi.org/10.69554/ogjs4246.
[213] Salomon, J. (2022). Public-Private Partnerships and Collective Cyber Defence. *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon)*, 700, 45-63. https://doi.org/10.23919/cycon55549.2022.9810912.
[214] Kesarwani, A., & Gochhayat, S. (2023). Ransomware Attacks in the Healthcare Industry. *Journal of Student Research*. https://doi.org/10.47611/jsrhs.v12i4.5799.

wpłynąć na globalne rynki finansowe. Inwestorzy doceniają takie proaktywne podejście do zarządzania ryzykiem, co może pozytywnie wpływać na wycenę akcji przedsiębiorstw zaangażowanych w tego typu inicjatywy. Kolejnym aspektem współpracy międzysektorowej jest jej wpływ na standaryzację najlepszych praktyk w cyberbezpieczeństwie. Organizacje takie jak ISAC często opracowują wytyczne i protokoły, które stają się punktem odniesienia dla całej branży. Na przykład FS-ISAC w swoim raporcie z 2021 roku opublikowało szczegółowe rekomendacje dotyczące ochrony przed atakami typu „*zero-day*", które zostały następnie wdrożone przez większość instytucji finansowych w Stanach Zjednoczonych[215]. W dłuższej perspektywie takie działania podnoszą ogólny poziom bezpieczeństwa w sektorze, co zwiększa zaufanie do rynku jako całości. Firmy uczestniczące w tych inicjatywach zyskują także wizerunek odpowiedzialnych i innowacyjnych graczy, co może przyciągać kapitał od inwestorów poszukujących stabilnych i przyszłościowych inwestycji.

Długoterminowe strategie cyberbezpieczeństwa wymagają od przedsiębiorstw ciągłego dostosowywania się do ewoluujących zagrożeń, co nie byłoby możliwe bez inwestycji w nowoczesne technologie. Kluczową rolę odgrywają tu systemy oparte na sztucznej inteligencji (AI) i uczeniu maszynowym (ML), które umożliwiają analizę ogromnej liczby danych w czasie rzeczywistym, wykrywanie anomalii i automatyczne reagowanie na incydenty. Algorytmy ML, takie jak sieci neuronowe czy modele predykcyjne oparte na analizie bayesowskiej, są w stanie identyfikować subtelne wzorce ataków, które umykają tradycyjnym metodom opartym na sygnaturach[216]. Inwestycje w technologie adaptacyjne, takie jak autonomiczne systemy obronne czy zaawansowane firewalle nowej generacji (NGFW), zwiększają również efektywność operacyjną, automatyzując procesy reagowania na zagrożenia i redukując obciążenie zespołów IT. Nie można jednak zapominać o wyzwaniach związanych z tymi technologiami. Wdrożenie systemów AI i ML wymaga znacznych nakładów finansowych. Ponadto skuteczność tych systemów zależy od jakości danych, na których są trenowane – błędne lub niekompletne dane mogą prowadzić do fałszywych alarmów lub przeoczenia rzeczywistych zagrożeń. Mimo tych wyzwań korzyści płynące z inwestycji w technologie adaptacyjne są niepodważalne. Firmy, które je wdrażają, zyskują nie tylko ochronę przed

[215] FS-ISAC. (2022). *Navigating Cyber 2022: A Complex Web of Cyber Risk*. https://www.fsisac.com/navigatingcyber2022-report

[216] Schmitt M., *Securing the Digital World: Protecting Smart Infrastructures and Digital Industries with Artificial Intelligence-enabled Malware and Intrusion Detection*, arXiv preprint, 2023.

cyberatakami, ale także przewagę konkurencyjną, demonstrując inwestorom i klientom swoją gotowość na wyzwania cyfrowej przyszłości[217].

Choć technologie odgrywają kluczową rolę w cyberbezpieczeństwie, to czynnik ludzki pozostaje najsłabszym ogniwem w systemie obronnym przedsiębiorstw. Błąd ludzki – taki jak otwarcie złośliwego załącznika, ujawnienie haseł w wyniku *phishingu* czy nieprzestrzeganie procedur bezpieczeństwa – jest przyczyną ponad 90% cyberataków[218]. Dlatego budowanie kultury bezpieczeństwa w organizacji, obejmującej regularne szkolenia, symulacje ataków i promowanie świadomości zagrożeń, jest niezbędnym elementem długoterminowej strategii cyberbezpieczeństwa. Szkolenia pracowników powinny być dostosowane do specyfiki ich stanowisk i regularnie aktualizowane w odpowiedzi na nowe zagrożenia. Kultura bezpieczeństwa ma także wymiar zewnętrzny – firmy, które promują ją jako integralną część swojej działalności, budują wizerunek odpowiedzialnych i godnych zaufania podmiotów. Jest to szczególnie istotne w oczach inwestorów, którzy coraz częściej zwracają uwagę na czynniki uwzględniane w podejściu ESG (*Environmental, Social, Governance*), w tym na zarządzanie ryzykiem cyfrowym[219].

W skali globalnej cyberbezpieczeństwo przyczynia się również do stabilności systemu finansowego, co jest kluczowe dla utrzymania zaufania do rynków. Ataki na instytucje finansowe, takie jak włamanie do systemu bankowego Bangladeszu w 2016 roku, które doprowadziło do kradzieży 81 milionów dolarów, pokazują, jak poważne mogą być konsekwencje braku odpowiednich zabezpieczeń[220]. Firmy, które inwestują w cyberbezpieczeństwo, nie tylko minimalizują ryzyko takich incydentów, ale także budują markę odpowiedzialnego i innowacyjnego podmiotu, co daje im przewagę konkurencyjną w oczach inwestorów i klientów.

---

[217] Jokic, A., Šarac, M., & Adamovic, S. (2023). Next-generation Firewall and Artificial Intelligence. *Proceedings of the International Scientific Conference - Sinteza 2023*. https://doi.org/10.15308/sinteza-2023-36-43.

[218] Mimecast, *The State of Human Risk 2025 – Report based on interviews with 1 100 IT security and IT decision-makers*, Mimecast Ltd., Londyn 2025.

[219] Aksoy, C. (2024). BUILDING A CYBER SECURITY CULTURE FOR RESILIENT ORGANIZATIONS AGAINST CYBER ATTACKS. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*. https://doi.org/10.33416/baybem.1374001.

[220] Mazumder, M., & Sobhan, A. (2020). The Spillover Effect of the Bangladesh Bank Cyber Heist on Banks' Cyber Risk Disclosures in Bangladesh. *Journal of Operational Risk*. https://doi.org/10.21314/JOP.2020.249.

Długoterminowe strategie cyberbezpieczeństwa są fundamentem budowania odporności rynkowej przedsiębiorstw w XXI wieku. Poprzez przestrzeganie regulacji prawnych, takich jak RODO, NIS2 czy DORA, firmy zapewniają sobie stabilność i unikają kar finansowych, jednocześnie zwiększając zaufanie inwestorów. Współpraca międzysektorowa, realizowana przez organizacje takie jak FS-ISAC, pozwala na skuteczne przeciwdziałanie globalnym zagrożeniom, wzmacniając stabilność całych sektorów gospodarki. Inwestycje w technologie adaptacyjne, takie jak sztuczna inteligencja i uczenie maszynowe, umożliwiają dynamiczną ochronę przed ewoluującymi atakami, podczas gdy budowanie kultury bezpieczeństwa redukuje ryzyko związane z błędami ludzkimi. Wszystkie te elementy razem przekładają się na lepszą pozycję rynkową firmy, jej większą konkurencyjność i zdolność do przyciągania kapitału inwestycyjnego. W świecie, w którym cyberzagrożenia stają się coraz bardziej złożone i powszechne, cyberbezpieczeństwo przestaje być jedynie kosztem operacyjnym – staje się strategiczną inwestycją w stabilność, rozwój i przyszłość przedsiębiorstwa na globalnym rynku.

Wnioski i podsumowanie

W niniejszej dysertacji autor skoncentrował się na analizie wpływu cyberataków na rynki finansowe oraz roli cyberbezpieczeństwa w zapewnieniu stabilności i konkurencyjności przedsiębiorstw w dobie cyfryzacji gospodarki. Współczesny świat biznesu, w którym dane i systemy informatyczne stanowią podstawę funkcjonowania większości firm, narażony jest na coraz bardziej wyrafinowane i powszechne cyberzagrożenia. Celem pracy było nie tylko zidentyfikowanie i przeanalizowanie bezpośrednich, krótkoterminowych skutków cyberataków na wartość rynkową przedsiębiorstw, ale także podkreślenie, w jaki sposób długoterminowe strategie w zakresie cyberbezpieczeństwa mogą przyczyniać się do wzmacniania ich pozycji rynkowej i budowania zaufania inwestorów. Wnioski płynące z badania, bazujące na przeglądzie literatury, analizie empirycznej, oraz analizie konkretnych przypadków oferują praktyczne rekomendacje dla przedsiębiorstw, inwestorów i regulatorów.

Po przeprowadzonych badaniach autor dowiódł, że cyberataki wywierają istotnie negatywny wpływ na krótkoterminową wartość rynkową firm notowanych na giełdzie. Przeprowadzona analiza skumulowanych nadzwyczajnych zwrotów (CAR) na podstawie 32 incydentów cybernetycznych w okresie od 2010 do 2024 roku wykazała, że średni CAR w oknie zdarzenia (-3, +3) wynosił -2,52%. Wynik ten, potwierdzony testem statystycznym t-Studenta ($t = -2{,}18$, $p < 0{,}05$), wskazuje na wyraźną negatywną reakcję rynku na ujawnienie cyberataku. Inwestorzy traktują takie incydenty jako sygnał zwiększonego ryzyka, co prowadzi do natychmiastowego spadku cen akcji w krótkim okresie po zdarzeniu. Uzyskane rezultaty są spójne z wcześniejszymi badaniami, m.in. Garga, Curtisa i Halpera (2003) oraz Campbella i in. (2003)[221][222], które również dokumentowały negatywne reakcje rynkowe na naruszenia bezpieczeństwa danych.

Przykłady spektakularnych incydentów, takich jak atak na Equifax, czy atak na SolarWinds, ilustrują, że w przypadku poważnych cyberataków reakcja rynku może być

[221] Garg A., Curtis J., Halper H., *The Financial Impact of IT Security Breaches: What Do Investors Think?*, *Information Systems Security*, t. 12(1), 2003, s. 22–33

[222] Campbell K., Gordon L. A., Loeb M. P., Zhou L., *The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market*, *Journal of Computer Security*, t. 11, 2003, s. 431–448

wyjątkowo silna[223][224]. Nawet w mniej dramatycznych przypadkach średni spadek CAR o 2,52% podkreśla powszechne zagrożenie dla akcjonariuszy w erze cyfrowej. Mechanizmem napędzającym te spadki jest utrata zaufania inwestorów, wynikająca z obaw o przyszłe straty finansowe, potencjalne kary regulacyjne, utratę klientów oraz koszty związane z odbudową infrastruktury i reputacji. Warto podkreślić, że skala strat rynkowych nie ogranicza się wyłącznie do bezpośrednich kosztów incydentu. Cyberataki generują efekt kaskadowy, wpływając na postrzeganie firmy jako stabilnego i wiarygodnego podmiotu gospodarczego. W efekcie przedsiębiorstwa dotknięte incydentami mogą zmagać się z podwyższonym kosztem kapitału oraz trudnościami w pozyskiwaniu nowych inwestorów czy utrzymaniu lojalności klientów. Wyniki te wskazują, że cyberzagrożenia mają charakter systemowy i wymagają kompleksowego podejścia do zarządzania ryzykiem.

Analiza wykazała znaczne zróżnicowanie reakcji rynku na poszczególne cyberataki, co sugeruje, że ich wpływ na wartość rynkową zależy od szeregu czynników kontekstowych. Najsilniejsze spadki wartości odnotowano w przypadkach incydentów o dużej skali i poważnych konsekwencjach reputacyjnych, takich jak wspomniane Equifax i SolarWinds. W tych sytuacjach rynek reagował gwałtownie, odzwierciedlając obawy o długoterminowe skutki dla działalności firm. Z kolei w niektórych przypadkach reakcja rynku była pozytywna, co odbiega od ogólnego trendu. Na przykład w przypadku Tesli atak nie wpłynął negatywnie na kluczowe operacje firmy, a szybka i skuteczna reakcja została odebrana jako dowód jej odporności. Podobnie firma Maersk, mimo ataku NotPetya w 2017 roku, odnotowała pozytywny CAR, co można przypisać efektywnej odbudowie działalności i minimalizacji strat operacyjnych.

To zróżnicowanie wskazuje, że reakcja rynku nie jest wyłącznie funkcją samego wystąpienia cyberataku, lecz zależy od takich elementów jak:

• Skala i charakter ataku – intensywność reakcji rynkowej jest ściśle związana z zakresem i naturą incydentu. Najsilniejsze spadki wartości rynkowej odnotowano w przypadkach masowych naruszeń danych klientów lub ataków na infrastrukturę krytyczną. Przykładem jest

[223] SolarWinds Corporation, *Form 10-K (rok 2020): ujawnienia dot. „Cyber Incident" (SUNBURST)*, 2021

[224] U.S. Securities and Exchange Commission (SEC), *Press Release 2023-227: SEC Charges SolarWinds…*, 30 X 2023

atak na British Airways (2018), w wyniku którego wyciekły dane finansowe ok. 400 tys. klientów, co przełożyło się na spadek CAR = –8,19%. Podobnie atak na Maersk (2017), wykorzystujący złośliwe oprogramowanie NotPetya i paraliżujący operacje w 76 portach, spowodował znaczne zakłócenia w łańcuchach dostaw i krótkotrwały spadek wyceny spółki.

• Efektywność zarządzania kryzysowego – szybka i skoordynowana reakcja może znacząco złagodzić negatywny wpływ cyberataku. Przypadek Anthem (2015) pokazuje, że natychmiastowe uruchomienie planu reagowania na incydent, w tym powiadomienie klientów i zaoferowanie im monitoringu kredytowego, ograniczyło spadek wartości rynkowej (CAR = –4,19%) oraz straty reputacyjne. Z kolei Adobe (2013), dzięki szybkiemu powiadomieniu użytkowników i wdrożeniu środków ochronnych, utrzymało relatywnie stabilny kurs akcji po ujawnieniu incydentu.

• Transparentność komunikacji – otwarte informowanie o incydencie, jego skutkach oraz działaniach naprawczych zmniejsza ryzyko utraty zaufania inwestorów. W tym kontekście pozytywnie wyróżnia się Maersk (2017), który prowadził regularną, rzeczową komunikację z mediami i partnerami, co ograniczyło wahania kursu i przyspieszyło odbudowę reputacji. Odmienny przykład stanowi Equifax (2017) – opóźnione ujawnienie informacji i brak przejrzystości w pierwszej fazie kryzysu przyczyniły się do silniejszej, długotrwałej reakcji rynku (CAR = –19,38%).

• Znaczenie incydentu dla operacji – ataki uderzające w podstawowe procesy biznesowe wywołują silniejsze efekty niż zdarzenia o charakterze peryferyjnym. SolarWinds (2020) doświadczył ataku na łańcuch dostaw, który objął tysiące klientów korporacyjnych i instytucji publicznych, co przełożyło się na największy spadek w całej próbie (CAR = –26,10%). W przeciwieństwie do tego, incydenty o ograniczonym zasięgu, jak Tesla (2018), dotyczące prób infiltracji wewnętrznej bez poważnych skutków operacyjnych, miały marginalny lub wręcz pozytywny wpływ na notowania (CAR = +7,52%).

Wyniki te zachęcają do prowadzenia dalszych badań nad determinantami reakcji rynkowych, szczególnie w kontekście różnic międzysektorowych i typów cyberataków (np. *ransomware*, *phishing*, ataki APT). Podkreślają również, że przedsiębiorstwa mają realny wpływ na percepcję rynku poprzez swoje działania w trakcie i po incydencie.

Przeprowadzone badanie potwierdza, że cyberbezpieczeństwo powinno być traktowane jako integralna część strategii zarządzania ryzykiem finansowym w przedsiębiorstwach. Negatywne wartości CAR po ujawnieniu cyberataku wskazują, że incydenty te wiążą się z wymiernymi stratami dla akcjonariuszy, co wpływa na koszt kapitału, stabilność finansową i zdolność do generowania zysków w przyszłości. W tym kontekście inwestycje w nowoczesne technologie ochrony danych, takie jak systemy SIEM (*Security Information and Event Management*), EDR (*Endpoint Detection and Response*) czy zapory sieciowe nowej generacji (NGFW) są nie tylko środkiem prewencji, ale także narzędziem ochrony wartości rynkowej. Przykłady takie jak atak na firmę Anthem Inc. w 2015 roku pokazują, że skuteczne procedury zarządzania kryzysowego – obejmujące szybkie powiadomienie interesariuszy, odzyskiwanie danych i komunikację z rynkiem – mogą znacząco ograniczyć straty finansowe i reputacyjne firmy. Z kolei brak odpowiednich działań, jak w przypadku firmy Marriott w 2018 roku, gdzie wyciek danych 500 milionów klientów skutkował długotrwałym spadkiem wartości rynkowej, prowadzi do pogłębienia kryzysu wizerunkowego. Analiza tych przypadków sugeruje, że proaktywne podejście do cyberbezpieczeństwa – w tym regularne testy penetracyjne, aktualizacje systemów i plany ciągłości działania – jest kluczowe dla minimalizacji skutków incydentów.

Co więcej, cyberbezpieczeństwo powinno być traktowane jako element strategiczny organizacji, wykraczający poza ochronę technologiczną. Firmy, które traktują je jako priorytet, budują wizerunek odpowiedzialnych i przewidujących podmiotów, co zwiększa ich atrakcyjność dla inwestorów i partnerów biznesowych. W erze, w której cyfrowe aktywa stają się równie cenne jak fizyczne, brak odpowiednich zabezpieczeń może być postrzegany jako zaniedbanie obowiązków zarządczych, co dodatkowo potęguje negatywne konsekwencje rynkowe. Wyniki badania podkreślają kluczową rolę regulacji prawnych w kształtowaniu standardów cyberbezpieczeństwa. Przepisy takie jak RODO[225] (Ogólne Rozporządzenie o Ochronie Danych), dyrektywa NIS2[226] czy DORA[227] (*Digital Operational Resilience Act*) nie

[225] Parlament Europejski i Rada UE, *Rozporządzenie (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO)*, Dz.U. UE L 119 z 4.5.2016, s. 1–88.

[226] Parlament Europejski i Rada UE, *Dyrektywa (UE) 2022/2555 z dnia 14 grudnia 2022 r. (NIS2)*, Dz.U. UE L 333 z 27.12.2022, s. 80–152. *(uzupełnia wymogi raportowania i zarządzania incydentami)*

[227] Parlament Europejski i Rada UE, *Rozporządzenie (UE) 2022/2554 z dnia 14 grudnia 2022 r. (DORA) w sprawie cyfrowej odporności operacyjnej sektora finansowego*, Dz.U. UE L 333 z 27.12.2022, s. 1–102.

tylko nakładają na przedsiębiorstwa obowiązek wdrażania odpowiednich zabezpieczeń, ale także wymuszają przejrzystość i odpowiedzialność w przypadku incydentów. Firmy przestrzegające tych regulacji unikają kar finansowych, które w niektórych przypadkach sięgają dziesiątek milionów euro (np. kara dla British Airways w wysokości 20 milionów GBP w 2020 roku), a jednocześnie budują wizerunek stabilnych i godnych zaufania podmiotów. Dla inwestorów przestrzeganie regulacji jest sygnałem, że firma minimalizuje ryzyko prawne i operacyjne, co pozytywnie wpływa na jej wycenę rynkową.

Równie istotna jest współpraca międzysektorowa, realizowana poprzez organizacje takie jak np. FS-ISAC (*Financial Services Information Sharing and Analysis Center*). Dzielenie się informacjami o zagrożeniach i najlepszych praktykach pozwala przedsiębiorstwom na szybsze reagowanie na nowe typy ataków i wzmacnianie ich odporności[228]. Przykłady globalnych kampanii cybernetycznych, takich jak WannaCry czy NotPetya pokazują, że zagrożenia cyfrowe mają charakter transgraniczny i wymagają skoordynowanych działań na poziomie sektorowym i międzynarodowym. Współpraca ta przyczynia się nie tylko do podnoszenia standardów bezpieczeństwa w poszczególnych firmach, ale także do zwiększenia stabilności rynków finansowych jako całości. Długoterminowa odporność na cyberzagrożenia wymaga od przedsiębiorstw inwestycji w nowoczesne technologie, takie jak sztuczna inteligencja (AI) i uczenie maszynowe (ML), które umożliwiają wykrywanie i neutralizowanie ataków w czasie rzeczywistym. Systemy oparte na AI, stosowane przez liderów rynku takich jak Palo Alto Networks czy Goldman Sachs, pozwalają na dynamiczną adaptację do ewoluujących zagrożeń, takich jak ataki zero-day czy zaawansowane kampanie APT (Advanced Persistent Threats). Jednocześnie technologie te redukują czas reakcji na incydenty, co jest kluczowe dla ograniczenia strat operacyjnych i finansowych.

Równie ważnym elementem jest budowanie kultury bezpieczeństwa w organizacji. Błędy ludzkie, takie jak kliknięcie w link phishingowy czy niewłaściwe zarządzanie hasłami, pozostają jednym z najczęstszych źródeł cyberataków. Regularne szkolenia, symulacje ataków i wdrażanie zasad bezpieczeństwa na wszystkich szczeblach organizacji są niezbędne dla

[228] S-ISAC (Financial Services Information Sharing and Analysis Center), *About Us / FAQ / Intelligence*, 2023–2025 (rola współdzielenia informacji i odporności sektora finansowego)

minimalizacji tego ryzyka. Inwestycje te mogą przekładać się na wymierne korzyści finansowe, w tym wzrost wartości rynkowej i przyciąganie kapitału.

Pomimo istotnych ustaleń, przeprowadzona analiza napotyka pewne ograniczenia, które należy uwzględnić przy interpretacji wyników. Po pierwsze, próba badawcza obejmująca 32 przypadki cyberataków, choć wystarczająca do uzyskania statystycznie istotnych rezultatów, pozostaje stosunkowo niewielka w porównaniu z badaniami analizującymi setki zdarzeń. Ogranicza to możliwość pełnej generalizacji wniosków na całą populację firm notowanych na giełdzie, szczególnie z rynków o odmiennej strukturze informacyjnej i płynności. Po drugie, analiza koncentrowała się na krótkoterminowych skutkach w siedmiodniowym oknie zdarzenia (-3, +3), co pozwala uchwycić bezpośrednią reakcję rynku, lecz nie obejmuje potencjalnych długofalowych konsekwencji cyberataków, takich jak utrata klientów, koszty prawne, odszkodowania, długoterminowe skutki reputacyjne czy zmiany w politykach bezpieczeństwa i strategiach biznesowych. Po trzecie, brak szczegółowego podziału próby na sektory gospodarki oraz typy ataków ogranicza możliwość identyfikacji różnic w wrażliwości poszczególnych branż na określone zagrożenia. Zidentyfikowane ograniczenia stanowią jednocześnie punkt wyjścia do dalszych badań, wskazane byłoby rozszerzenie zakresu badania i jego perspektywy metodologicznej.

W szczególności:

- Dłuższy horyzont czasowy – analiza średnio- i długoterminowych skutków cyberataków (np. w okresach 30, 90 czy 180 dni po incydencie) pozwoliłaby ocenić trwałość reakcji rynku oraz proces odbudowy zaufania inwestorów. Włączenie długofalowych miar, takich jak Buy-and-Hold Abnormal Returns (BHAR), umożliwiłoby określenie, czy spadki wartości obserwowane w krótkim okresie są jedynie tymczasowe, czy też mają charakter trwały.
- Analiza sektorowa – porównanie reakcji rynku w różnych branżach, np. finansowej, technologicznej, transportowej czy przemysłowej, pozwoliłoby zidentyfikować sektory szczególnie podatne na incydenty cybernetyczne. Przykłady z obecnej próby (np. Maersk, British Airways, Equifax, Anthem) sugerują, że branże o dużym udziale danych osobowych lub o charakterze infrastrukturalnym reagują silniejszym spadkiem CAR.
- Wpływ regulacji – szczegółowe badanie roli ram prawnych, takich jak RODO, NIS2 czy DORA, mogłoby pokazać, jak otoczenie regulacyjne wpływa na percepcję ryzyka

przez inwestorów. Analizy porównawcze pomiędzy incydentami sprzed i po wejściu w życie kluczowych regulacji mogłyby ujawnić, czy wzrost przejrzystości i obowiązek raportowania zdarzeń rzeczywiście łagodzą negatywne reakcje rynku.

- Typologia ataków i skuteczność reakcji – zróżnicowanie reakcji rynku w zależności od charakteru ataku (np. ransomware, data breach, supply chain attack) oraz jakości reakcji przedsiębiorstwa (czas detekcji, komunikacja kryzysowa, odzyskiwanie systemów) może dostarczyć bardziej precyzyjnych wniosków dotyczących mechanizmów kształtujących zachowania inwestorów. Przykłady takich różnic widoczne są w reakcji rynku na ataki o podobnej skali, lecz odmiennym przebiegu zarządzania kryzysem – np. bardziej umiarkowana reakcja w przypadku Anthem w porównaniu z Equifax.

Uwzględnienie powyższych aspektów w przyszłych analizach pozwoliłoby poszerzyć zrozumienie zależności między cyberatakami a reakcją rynków finansowych, a także lepiej ocenić, jak czynniki operacyjne, regulacyjne i komunikacyjne kształtują proces odzyskiwania wartości przedsiębiorstw po incydentach bezpieczeństwa. Podsumowując, cyberataki stanowią istotne zagrożenie dla wartości rynkowej przedsiębiorstw, co potwierdzają ujemne skumulowane nadzwyczajne zwroty (średni CAR = -2,52%) obserwowane po ujawnieniu incydentów. Wyniki badania podkreślają, że cyberbezpieczeństwo jest nieodzownym elementem zarządzania ryzykiem finansowym i strategii biznesowej w dobie cyfryzacji. Przedsiębiorstwa, które inwestują w nowoczesne technologie, przestrzegają regulacji prawnych, budują kulturę bezpieczeństwa i angażują się we współpracę międzysektorową, mogą nie tylko minimalizować ryzyko związane z cyberatakami, ale także wzmacniać swoją pozycję na rynkach finansowych, budując zaufanie inwestorów i klientów. W kontekście rosnących zagrożeń cyfrowych i globalnej zależności od technologii, cyberbezpieczeństwo staje się kluczowym czynnikiem determinującym sukces i stabilność współczesnych przedsiębiorstw.

BIBLIOGRAFIA

A. Monografie, artykuły naukowe i materiały konferencyjne (w tym książki/podręczniki)

Aivazpour, Z., Valecha, R., Chakraborty, R., Data Breaches, ACM SIGMIS Database, 53, 2022, s. 65–82. https://doi.org/10.1145/3571823.3571829

Akyildirim, E., Conlon, T., Corbet, S., Hou, Y., HACKED: Understanding the Stock Market Response to Cyberattacks, Journal of Economic Behavior & Organization, 2024. https://doi.org/10.1016/j.jebo.2024.106423

Aljaidi, M., A Comprehensive Technical Analysis of URL Redirect Attacks: A Case Study of British Airways Data Breach, ACIT 2023, 2023, s. 1–5. https://doi.org/10.1109/ACIT58888.2023.10453784

Alkhalil, Z., Hewage, C., Nawaf, L., Khan, I., Phishing Attacks: A Recent Comprehensive Study and a New Anatomy, Frontiers in Computer Science, 3, 2021, art. 563060. https:/doi.org/10.3389/fcomp.2021.563060

Arcuri, M. C., Brogi, M., Gandolfi, G., The Effect of Cyber-Attacks on Stock Returns, Corporate Ownership & Control, 15(2), 2018, s. 70–83. https://doi.org/10.22495/cocv15i2art6

Bacidore, J. M., Wu, D., Xu, W., Balancing Execution Risk and Trading Cost in Portfolio Trading Algorithms, The Journal of Trading, 8(4), 2013, s. 37–43. https://doi.org/10.3905/jot.2013.8.4.037

Babych, O., Digitalisation of Financial Markets, Current Issues, and Challenges, State and Regions. Series: Economics and Business, 2023. https://doi.org/10.32782/1814-1161/2023-3-1

Bharadwaj, Y., Bhageerath, Y., Cyber Security, Challenges, Some Practical Solutions, IJSR CSEIT, 2019. https://doi.org/10.32628/CSEIT19519

Bjønnes, G. H., Rime, D., Solheim, H. O., The Impact of Different Players on the Volume-Volatility Relation in the Foreign Exchange Market, Beta, 2019. https://doi.org/10.18261/ISSN.1504-3134-2019-01-04

Blazhevich, O., Safonova, N. S., Features of the Financial Market Development in the Conditions of Digitalization, Scientific Bulletin: Finance, Banking, Investment, 2022. https://doi.org/10.37279/2312-5330-2021-1-106-124

Bridges, R., Rice, A. E., Oesch, S., Nichols, J. A., Watson, C., Spakes, K. D., Testing SOAR Tools in Use, arXiv, 2022. https://doi.org/10.48550/arXiv.2208.06075

Brown, S. J., Warner, J. B., Using Daily Stock Returns: The Case of Event Studies, Journal of Financial Economics, 14(3), 1985, s. 3–31.

Campbell, J. Y., Lo, A. W., MacKinlay, A. C., The Econometrics of Financial Markets, Princeton University Press, Princeton 1997, s. 149–180. https://doi.org/10.1515/9781400830213

Campbell, K., Gordon, L. A., Loeb, M. P., Zhou, L., The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market, Journal of Computer Security, 11, 2003, s. 431–448.

Carrapico, H., Farrand, B., Cybersecurity Trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics, JCMS, 2024. https://doi.org/10.1111/jcms.13654

Carrillo, E. F. P., Cybersecurity in European Financial Institutions: New Grounds for Corporate Governance Reform, European Business Law Review, 2023.

Cartea, Á., Jaimungal, S., Wang, Y., Spoofing and Price Manipulation in Order-Driven Markets, Applied Mathematical Finance, 27(1), 2020, s. 67–98. https://doi.org/10.1080/1350486X.2020.1726783

Corbet, S., Larkin, C., Lucey, B., HACKED: Understanding the Stock Market Response to Cyberattacks, Finance Research Letters, 2023. https://doi.org/10.1016/j.frl.2023.104206

Cornish, P., The Cybersecurity Lexicon, Routledge, 2017.

Daiya, H., AI-Driven Risk Management Strategies in Financial Technology, JAIGS, 2024. htts://doi.org/10.60087/jaigs.v5i1.194

Deshpande, A. S., Cybersecurity in Financial Services: Addressing AI-Related Threats and Vulnerabilities, ICKECS 2024, 2024, s. 1–6. https://doi.org/10.1109/ICKECS61492.2024.10616498

Deshpande, A. S., Regulatory Compliance and AI: Navigating the Legal and Regulatory Challenges of AI in Finance, ICKECS 2024, 2024, s. 1–5. https://doi.org/10.1109/ICKECS61492.2024.10616752

Easley, D., López de Prado, M. M., O'Hara, M., The Microstructure of the "Flash Crash", The Journal of Portfolio Management, 37(2), 2011, s. 118–128. https://doi.org/10.3905/jpm.2011.37.2.118

Enoma, B., Data Breach in the Travel Sector and Strategies for Risk Mitigation, Journal of Data Protection & Privacy, 2020.

Erkan-Barlow, A., Ngo, T., Goel, R., Streeter, D., An In-Depth Analysis of the Impact of Cyberattacks on the Profitability of Commercial Banks in the United States, Journal of Global Business Insights, 8(2), 2023. https://doi.org/10.5038/2640-6489.8.2.1246

Eze, C., Shamir, L., Analysis and Prevention of AI-Based Phishing Email Attacks, IEEE Access, 12, 2024, s. 31745–31759. https://doi.org/10.1109/ACCESS.2024.3390213

Fama, E. F., Market Efficiency, Long-Term Returns, and Behavioral Finance, Journal of Financial Economics, 49(2), 1998, s. 283–306.

Ferreira, J., Ribeiro, P., Pereira, T., Vishing and Smishing Threats…, Journal of Information Security and Applications, 70, 2023, art. 103517. https://doi.org/10.1016/j.jisa.2023.103517

Ford, A., Al-Nemrat, A., Ghorashi, S., Davidson, J., The Impact of GDPR Infringement Fines on the Market Value of Firms, Information & Computer Security, 31, 2022, s. 51–64. https://doi.org/10.1108/ICS-03-2022-0049

Garg, A., Curtis, J., Halper, H., The Financial Impact of IT Security Breaches: What Do Investors Think?, Information Systems Security, 12(1), 2003, s. 22–33.

Gatzert, N., Martin, M., The Impact of Cyber Risks on Capital Markets – An Empirical Event Study, European Actuarial Journal, 12, 2022, s. 157–185. https://doi.org/10.1007/s13385-021-00294-

Geers, K., Strategic Cyber Security, NATO CCDCOE, 2011.

Geisler, K., Hacking Wall Street: Reconceptualizing Insider Trading Law for Computer Hacking and Trading Schemes, White Collar Crime eJournal, 2018. https://doi.org/10.2139/ssrn.3221987

Gilderdale, S., SWIFT's Customer Security Programme…, Journal of Securities Operations & Custody, 2017. https://doi.org/10.69554/eicr3197

Gontareva, I., Chorna, M., Pawliszczy, D., i in., Features of the Entrepreneurship Development in Digital Economy, TEM Journal, 7(4), 2018, s. 857–868. https://doi.org/10.18421/tem74-19

Havakhor, T., Rahman, M., Zhang, T., Disclosure of Cybersecurity Investments and the Cost of Capital, SSRN, 2021. https://doi.org/10.2139/ssrn.3553470

Havryk, A., Nazarova, T., Artificial Intelligence and its Role in the Labor Market and Financial Sector…, ISJMEF, 2024. https://doi.org/10.46299/j.isjmef.20240303.01

Himma, K. E., The Ethics of Cybersecurity, Springer, 2021.

Hoehle, H., Wei, J., Schuetz, S., Venkatesh, V., User Compensation as a Data Breach Recovery Action…, Internet Research, 31, 2021, s. 765–781. https://doi.org/10.1108/INTR-02-2020-0105

Hutchins, E. M., Cloppert, M. J., Amin, R. M., Intelligence-Driven Computer Network Defense… Kill Chains, Lockheed Martin, 2011.

Inns, J., The Evolution and Application of SIEM Systems, Network Security, 2014(9), s. 16–17. https://doi.org/10.1016/S1353-4858(14)70051-0

Jaiwani, M., Gopalkrishnan, S., i in., The Blockchain Revolution… Derivative Markets, ICTMOD 2023, 2023, s. 1–7. https://doi.org/10.1109/ICTMOD59086.2023.10438145

Jasper, S., North Korea's Cyberspace Aggression, International Journal of Intelligence and CounterIntelligence, 32(2), 2019, s. 194–198.

Jokic, A., Šarac, M., Adamovic, S., Next-generation Firewall and Artificial Intelligence, Sinteza 2023, 2023, s. 36–43. https://doi.org/10.15308/sinteza-2023-36-43

Kadivar, M., Cyber-Attack Attributes…, Technology Innovation Management Review, 4(11), 2014.

Karimi, A., Niyaz, Q., Sun, W., Javaid, A., Devabhaktuni, V., Distributed Network Traffic Feature Extraction for a Real-Time IDS, IEEE EIT 2016, 2016, s. 522–526. https://doi.org/10.1109/EIT.2016.7535295

Kathiresan, V., Karthik, S., Divya, P., Rajan, D., A Comparative Study of Diverse Intrusion Detection Methods…, ICCCI 2022, 2022, s. 1–6. https://doi.org/10.1109/ICCCI54379.2022.9740744

Kesan, J., Hayes, C., Self Defense in Cyberspace: Law and Policy, 2011. (uzupełnij dane wydawnicze)

Kirilenko, A., Kyle, A. S., Samadi, M., Tuzun, T., The Flash Crash: High-Frequency Trading in an Electronic Market, SSRN, 2017. https://doi.org/10.2139/ssrn.1686004

Kopp, K., Kaffenberger, C., Wilson, M., Cyber Risk Measurement and the Holistic Impact of Cyberattacks, Journal of Cybersecurity, 3(1), 2017, s. 13.

Kothari, S. P., Warner, J. B., Econometrics of Event Studies, [w:] Eckbo, B. E. (red.), Handbook of Corporate Finance, Elsevier, Amsterdam 2006, s. 3–36. https://doi.org/10.1016/B978-0-444-53187-6.50002-8

Kowalski, M., Rekordowo wysokie koszty naruszeń danych – raport IBM, Computerworld Polska, 2021.

Kudła, J., Instrumenty finansowe i ich zastosowanie, Key Text, Warszawa 2022.

Lee, I., Lee, K., The Internet of Things (IoT): Applications…, Business Horizons, 58(4), 2015, s. 431–440. https://doi.org/10.1016/j.bushor.2015.03.008

Lei, S., Synergizing Next-Generation Firewalls and Defense-in-Depth Strategies…, Proc. SPIE, 13175, 2024, 131750M. https://doi.org/10.1117/12.3031957

Leonard, G., Cao, Y., Haas, M., Mocek, G., The Legal and Economic Implications from Recent UK Spoofing Cases, Journal of Financial Compliance, 2020.

Liang, Y., Kim, Y., Evolution of Firewalls… NGFW, IEEE CCWC 2022, 2022. https://doi.org/10.1109/CCWC54503.2022.9720435

Long, S. C., Lucey, B., Xie, Y., Yarovaya, L., "I Just Like the Stock": Reddit Sentiment and GameStop, Financial Review, 2022. https://doi.org/10.1111/fire.12328

Lv, Y., Data Privacy Protection Based on Homomorphic Encryption, J. Phys.: Conf. Ser., 2037, 2021. https://doi.org/10.1088/1742-6596/2037/1/012129

MacKinlay, A. C., Event Studies in Economics and Finance, Journal of Economic Literature, 35(1), 1997, s. 13–39.

Mahajan, S., Morya, S., Analysis of the Interplay of Hacking and Its Effects on Financial Market, Nanotechnology Perceptions, 20, 2024. https://doi.org/10.62441/nano-ntp.v20is9.53

Martin, K. D., Borah, A., Palmatier, R. W., A Strong Privacy Policy Can Save Your Company Millions, Harvard Business Review, 15 II 2018.

Mazumder, M., Sobhan, A., The Spillover Effect of the Bangladesh Bank Cyber Heist…, Journal of Operational Risk, 2020. https://doi.org/10.21314/JOP.2020.249

McCorry, P., Möser, M., Ali, S., Why Preventing a Cryptocurrency Exchange Heist Isn't Good Enough, [w:] FC & Data Security, 2018, s. 225–233. https://doi.org/10.1007/978-3-030-03251-7_27

Meland, P., Johansen, B., Sindre, G., An Experimental Analysis of Cryptojacking Attacks, 2019, s. 155–170. https://doi.org/10.1007/978-3-030-35055-0_10

Miljkovic, L., The Role of Financial Derivatives in Financial Risks Management, MEST Journal, 2023. https://doi.org/10.12709/mest.11.11.01.09

Min, B. H., Borch, C., Systemic Failures and Organizational Risk Management in Algorithmic Trading, Social Studies of Science, 52(2), 2021, s. 277–302. https://doi.org/10.1177/03063127211048515

Mirsky, S., Lee, W., The Emerging Threat of Deepfakes…, ACM SIGSAC, 2023. https://doi.org/10.1145/3584202.3584300

Mykhalchynets, H., Financial Market as a Basis…, Herald of Khmelnytskyi NU, 2023. https://doi.org/10.31891/2307-5740-2023-314-1-12

Nalini, R., Yuvasri, S., A Study on the Impact of Digital Transformation in the Banking Sector on Customer's Experience, IJIREM, 2024. https://doi.org/10.55524/ijirem.2024.11.2.8

Natarajan, H., Balakrishnan, M., Real-Time Retail Payments…, Journal of Payments Strategy & Systems, 2020.

Novak, O., Osadcha, T., Petruk, O., Concept and Classification of Derivative Financial Instruments…, Baltic Journal of Economic Studies, 2019. https://doi.org/10.30525/2256-0742/2019-5-3-135-144

Nurusheva, A., Medelbayeva, N., Satybaldina, D., Goranin, N., Machine Learning Algorithms in SIEM Systems…, Bulletin of ENU, 2024. https://doi.org/10.32523/bulmathenu.2024/3.1

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., The Human Aspects of Information Security Questionnaire (HAIS-Q), Computers & Security, 66, 2017, s. 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Perols, R., The Impact of the Type of Cybersecurity Assurance Service…, Auditing: A Journal of Practice & Theory, 2023.

Pereira, C. M., Unregulated Algorithmic Trading…, Journal of Financial Regulation, 6(3), 2020, s. 270–305. https://doi.org/10.1093/jfr/fjaa008

Peter, I., Ijiga, M., Olajide, F. I., Olatunde, T. I., Harnessing Adversarial Machine Learning…, OARJST, 2024. https://doi.org/10.53022/oarjst.2024.11.1.0060

Plachkinova, M., Maurer, C., Teaching Case: Security Breach at Target, JISE, 29, 2018, s. 11–20.

Prasad, S., Role of Financial Innovations in Economic Development, 40, 2020, s. 133–136.

Priyadarshana, D., Rao, T. R., Rao, M. S., AI and Blockchain Technology for Secure and Transparent Financial Transactions, IJSRA, 2024. https://doi.org/10.30574/ijsra.2024.13.1.1845

Qureshi, N. I., Choudhuri, S. S., i in., Ethical Considerations of AI in Financial Services…, ICKECS 2024, 2024, s. 1–6. https://doi.org/10.1109/ICKECS61492.2024.10616483

Ramakrishnan, R., The Future of Cybersecurity and Its Potential Threats, IJRASET, 2023. https://doi.org/10.22214/ijraset.2023.54603

Rid, T., Cyber War Will Not Take Place, Oxford University Press, 2013.

Sasikumar, S., Sundaram, N., Event Study Methodology Trends in the Stock Market…, Multidisciplinary Reviews, 2024. https://doi.org/10.31893/multirev.2024234

Schmitt, M., Securing the Digital World… AI-enabled Malware and Intrusion Detection, arXiv, 2023.

Schroeder, F., Lepone, A., Leung, H., Satchell, S., Flash Crash in an OTC Market…, European Journal of Finance, 26(12), 2020, s. 1569–1589. https://doi.org/10.1080/1351847X.2020.1748893

Seo, J., Business Value of Blockchain and Applications of AI, Asia-Pacific Journal of Multimedia Services Convergent…, 8(7), 2018, s. 779–789. https://doi.org/10.35873/ajmahs.2018.8.7.076

Singer, P. W., Friedman, A., Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2014.

Subramanian, H., Security Tokens: Architecture, Smart Contract Applications and Illustrations Using SAFE, Managerial Finance, 45(4), 2019. https://doi.org/10.1108/MF-09-2018-0467

Su, Y., A Comprehensive Survey of DDoS Attacks and Defenses, Electronics, 13(4), 2024, art. 807. https://doi.org/10.3390/electronics13040807

Takebayashi, T., Tsuda, H., Hasebe, T., Masuoka, R., Data Loss Prevention Technologies, Fujitsu Scientific & Technical Journal, 46, 2010, s. 47–55.

Tosun, O. K., Cyber Attacks and Stock Market Activity, International Review of Financial Analysis, 76, 2021, art. 101795. https://doi.org/10.1016/j.irfa.2021.101795

Ullah, S., Zaefarian, G., Ahmed, R., Kimani, D., How to Apply the Event Study Methodology in STATA, Industrial Marketing Management, 2021. https://doi.org/10.1016/j.indmarman.2021.02.004

Vo, H. T. K., Wojciechowski, R., Weinhardt, C., Integration of Electronic Foreign Exchange Trading and Corporate Treasury Systems with Web Services, LNCS, 3795, 2005, s. 471–488. https://doi.org/10.1007/3-7908-1624-8_25

Von Solms, A., Von Solms, R., Information Security Governance, Springer, 2018.

Wang, J., Does Cybersecurity Risk Stifle Corporate Innovation Activities?, Journal of Corporate Finance, 76, 2024, s. 102212.

Wang, Q., Ngai, E., Event Study Methodology in Business Research: A Bibliometric Analysis, Industrial Management & Data Systems, 120, 2020, s. 1863–1900. https://doi.org/10.1108/IMDS-12-2019-0671

Wieland, I., Kovács, L., Savchenko, T., Conceptual Study of the Difference Between the Money Market and the Capital Market, Financial Markets, Institutions and Risks, 4(1), 2020, s. 51–59. https://doi.org/10.21272/fmir.4(1).51-59.2020

Wolff, J., Lehr, W., When Cyber Threats Loom, What Can State and Local Governments Do?, Georgetown Journal of International Affairs, 19, 2018, s. 67–75. https://doi.org/10.1353/GIA.2018.0008

Yavorska, V., Analysis of Capital Markets and Organized Commodity Markets, Market Infrastructure, 2022.

Yost, J. R., Computer Security [Guest Editors' Introduction], IEEE Annals of the History of Computing, 37(2), 2015, s. 6–7. https://doi.org/10.1109/MAHC.2015.33

B. Raporty i opracowania instytucjonalne

ENISA, Threat Landscape 2022: Cyber Threats and Trends, Publications Office of the European Union, 2022, s. 14–16.

FS-ISAC, Navigating Cyber 2022: A Complex Web of Cyber Risk, 2022. https://www.fsisac.com/navigatingcyber2022-report

Frontier Economics, Assessing the Economic Cost of EU Initiatives on Cybersecurity: The Impact of NIS2, 12 VII 2023.

IBM, Consumers Pay the Price as Data Breach Costs Reach All-Time High, IBM Newsroom, 27 VII 2022.

IBM, Cost of a Data Breach Report 2024 (w Twojej liście było „2043" – poprawiłem na 2024; proszę potwierdź edycję raportu).

KPMG, Barometr cyberbezpieczeństwa 2023/2024 (PL), 2024.

Microsoft, Digital Defense Report 2021, 2021.

Mimecast, The State of Human Risk 2025, Mimecast Ltd., Londyn 2025.

National Audit Office (UK), Investigation: WannaCry cyber attack and the NHS, 27 X 2017.

NIST, Advanced Encryption Standard (AES) – FIPS PUB 197, Gaithersburg, 2001.

Związek Cyfrowa Polska, Raport o stanie cyberbezpieczeństwa polskich firm 2021, 2021.

Ministerstwo Cyfryzacji (PL), Krajowy system cyberbezpieczeństwa – zadania i cele, Gov.pl, dostęp 20.11.2024.

C. Akty prawne

California State Legislature, California Consumer Privacy Act of 2018 (CCPA), California Civil Code §§ 1798.100–1798.199, Sacramento 2018 (z późn. zm. CPRA 2020).

Parlament Europejski i Rada UE, Rozporządzenie (UE) 2016/679 (RODO), Dz.U. UE L 119 z 4.5.2016, s. 1–88.

Parlament Europejski i Rada UE, Dyrektywa 2014/65/UE (MiFID II), Dz.U. UE L 173 z 12.6.2014, s. 349–496.

Parlament Europejski i Rada UE, Dyrektywa (UE) 2022/2555 (NIS2), Dz.U. UE L 333 z 27.12.2022, s. 80–152.

Parlament Europejski i Rada UE, Rozporządzenie (UE) 2022/2554 (DORA), Dz.U. UE L 333 z 27.12.2022, s. 1–102.

D. Komunikaty korporacyjne, dokumenty urzędowe

A. P. Møller – Mærsk, Cyber attack update, 28 VI 2017.

BankInfoSecurity, eBay Breach: 145 Million Users Notified, 21 V 2014.

California Department of Insurance, Consumer Information on Anthem Breach, 2015.

CISA, The Attack on Colonial Pipeline: What We’ve Learned…, 2023.

Cognizant, Security Incident Update, 18 IV 2020.

EC (SEC filing), Quest Diagnostics Statement on the AMCA Data Security Incident (8-K), 03 VI 2019.

SEC (U.S. Securities and Exchange Commission), Press Release 2023-227: SEC Charges SolarWinds…, 30 X 2023.

SolarWinds Corporation, Form 10-K (2020): Disclosure on “Cyber Incident” (SUNBURST), 2021.

E. Źródła prasowe i branżowe (media)

Byszewski, G., Kozubal, M., Nie działała strona giełdy. Atak hakerów?, Rzeczpospolita, 23 X 2014.

Cimpanu, C., Insurance Giant Aon Hit by a Cyberattack, BleepingComputer, 28 II 2022.

DarkReading, Toyota Halts Production After Suspected Supply Chain Attack, 01 III 2022.

Defense One, RSA Verifies Its Tokens Played Role in Lockheed Cyberattack, 07 VI 2011.

Dellinger, A. J., First American Financial Data Leak…, Forbes, 2019.

Ferguson, S., WannaCry… Boeing, Dark Reading, 29 III 2018.

Goldstein, M., MGM Resorts Data Breach…, Forbes, 20 II 2020.

HALOCK Security Labs, Pepsi Cola Bottler Falls Victim to a Data Breach, 10 II 2023.

HIPAA Journal, Flaw in Walgreens Mobile App…, 04 III 2020.

ICO (omówienie), BA Fined £20m, 2020, GDPRregister.eu.

Krebs, B., Adobe To Announce Source Code, Customer Data Breach, 03 X 2013.

Krebs, B., First American… Leaked Hundreds of Millions of Records, 24 V 2019.

Murphy, M., JPMorgan Data Breach Involves Information on 76 Million Households…, 2014.

PAP/TVN24, Amerykańskie służby odzyskały część okupu… (Colonial Pipeline), 2021.

Scimeca, D., Clorox Cyberattack Cost $356 Million, IndustryWeek, 05 X 2023.

TIME, Data Breach at [24]7.ai May Have Hit Delta, 05 IV 2018.

WIRED, The Untold Story of NotPetya…, 22 VIII 2018.

WIRED, Norsk Hydro Cyber Attack Is About Money, Not War, 20 III 2019.

Załączniki

Załącznik 1 – Nadzwyczajne zwroty w oknie zdarenia

Data	Nazwa firny	Stopa zwrotu	Oczekiwana stopa zwrotu	AR
30.09.2013	Adobe	-0,001729774	-0,006115568	0,44%
01.10.2013	Adobe	0,009433995	0,009322927	0,01%
02.10.2013	Adobe	-0,017356472	-0,000213714	-1,71%
03.10.2013	Adobe	-0,012422348	-0,00936244	-0,31%
04.10.2013	Adobe	0,013561293	0,00828254	0,53%
07.10.2013	Adobe	-0,014543339	-0,008841815	-0,57%
08.10.2013	Adobe	-0,024399801	-0,013052269	-1,13%
30.01.2015	Anthem	-0,015609071	-0,014142489	-0,15%
02.02.2015	Anthem	0,004001097	0,017062034	-1,31%
03.02.2015	Anthem	0,010774797	0,018837841	-0,81%
04.02.2015	Anthem	0,005038113	-0,00351923	0,86%
05.02.2015	Anthem	-0,003051436	0,013850672	-1,69%
06.02.2015	Anthem	-0,011221983	-0,002632098	-0,86%
09.02.2015	Anthem	-0,005969457	-0,003628815	-0,23%
23.02.2022	Aon	-0,01766615	-0,014977027	-0,27%
24.02.2022	Aon	0,028117565	0,012212382	1,59%
25.02.2022	Aon	0,016728608	0,018254874	-0,15%
28.02.2022	Aon	-0,00276484	-0,001964888	-0,08%
01.03.2022	Aon	-0,007873185	-0,012582608	0,47%
02.03.2022	Aon	0,010350715	0,015215641	-0,49%
03.03.2022	Aon	0,004678319	-0,004256188	0,89%
23.03.2018	Boeing	0,004348977	-0,024536822	2,89%
26.03.2018	Boeing	0,02482875	0,035921612	-1,11%
27.03.2018	Boeing	-0,023862426	-0,01990035	-0,40%

28.03.2018	Boeing	-0,003425411	-0,001860296	-0,16%
29.03.2018	Boeing	0,024560853	0,019102826	0,55%
02.04.2018	Boeing	-0,016591426	-0,026258637	0,97%
04.09.2018	British Airways	-0,03921565	-0,002576216	-3,66%
05.09.2018	British Airways	-0,030612276	-0,002919767	-2,77%
06.09.2018	British Airways	0	-0,003173714	0,32%
07.09.2018	British Airways	0,002631576	-0,002743392	0,54%
10.09.2018	British Airways	-0,036745372	-0,001513943	-3,52%
11.09.2018	British Airways	0,008174379	-0,000963087	0,91%
24.07.2019	Capital One	0,027348196	0,006833723	2,05%
25.07.2019	Capital One	-0,010524256	-0,006895055	-0,36%
26.07.2019	Capital One	0,022731957	0,010558285	1,22%
29.07.2019	Capital One	-0,011826914	-0,001864271	-1,00%
30.07.2019	Capital One	-0,058914615	-0,003192289	-5,57%
31.07.2019	Capital One	0,013266188	-0,014653284	2,79%
01.08.2019	Capital One	-0,012118705	-0,012050159	-0,01%
14.04.2020	Cognizant	0,025996091	0,035994928	-1,00%
15.04.2020	Cognizant	-0,039393337	-0,025666908	-1,37%
16.04.2020	Cognizant	-0,00904896	0,006975795	-1,60%
17.04.2020	Cognizant	0,045463494	0,03156515	1,39%
20.04.2020	Cognizant	-0,023787575	-0,020802948	-0,30%
21.04.2020	Cognizant	-0,029316348	-0,035799917	0,65%
22.04.2020	Cognizant	0,024906691	0,027036493	-0,21%
02.04.2018	Delta Airlines	-0,052180157	-0,021690141	-3,05%
03.04.2018	Delta Airlines	0,034071212	0,012645953	2,14%
04.04.2018	Delta Airlines	0,002606253	0,011616053	-0,90%
05.04.2018	Delta Airlines	0,006498044	0,006995356	-0,05%
06.04.2018	Delta Airlines	-0,021398053	-0,021280321	-0,01%
09.04.2018	Delta Airlines	-0,009236662	0,003531209	-1,28%
10.04.2018	Delta Airlines	-0,003805188	0,016685547	-2,05%
23.11.2016	Deutsche Telekom	-0,012469033	0,000161298	-1,26%

25.11.2016	Deutsche Telekom	0,014785285	0,001262412	1,35%
28.11.2016	Deutsche Telekom	0,018823622	-0,001987701	2,08%
29.11.2016	Deutsche Telekom	0	0,000348199	-0,03%
30.11.2016	Deutsche Telekom	-0,028287913	-0,001065676	-2,72%
01.12.2016	Deutsche Telekom	0,005585987	-0,001371274	0,70%
05.09.2017	Equifax	-0,003460623	-0,008107683	0,46%
06.09.2017	Equifax	0,002055445	0,003270771	-0,12%
07.09.2017	Equifax	0,00940662	-0,000252829	0,97%
08.09.2017	Equifax	-0,136561202	-0,001649003	-13,49%
11.09.2017	Equifax	-0,082041667	0,01148596	-9,35%
12.09.2017	Equifax	0,025105893	0,003521386	2,16%
09.05.2017	FedEx	-0,001674562	-0,002694056	0,10%
10.05.2017	FedEx	-0,005451158	0,000761132	-0,62%
11.05.2017	FedEx	0,005744743	-0,004517229	1,03%
12.05.2017	FedEx	0,004296648	-0,00342039	0,77%
15.05.2017	FedEx	0,016174496	0,006604449	0,96%
16.05.2017	FedEx	-0,003183373	-0,002151779	-0,10%
17.05.2017	FedEx	-0,034253558	-0,030185175	-0,41%
21.05.2019	First American	0,007642262	0,007075021	0,06%
22.05.2019	First American	0,00397219	-0,000621485	0,46%
23.05.2019	First American	-0,012949572	-0,006801513	-0,61%
24.05.2019	First American	0,006924087	0,002219063	0,47%
28.05.2019	First American	-0,062613075	-0,004395743	-5,82%
29.05.2019	First American	0,011969214	-0,003400544	1,54%
20.07.2020	Garmin	-0,002190878	0,00839366	-1,06%
21.07.2020	Garmin	-0,003892101	0,002294037	-0,62%
22.07.2020	Garmin	0,01542936	0,005982191	0,94%
23.07.2020	Garmin	-0,011346975	-0,010397589	-0,09%
24.07.2020	Garmin	-0,034530996	-0,004840522	-2,97%
27.07.2020	Garmin	0,036696484	0,007476346	2,92%
28.07.2020	Garmin	-0,009273102	-0,005097087	-0,42%

03.09.2014	Home Depot	-0,023587407	0,000329756	-2,39%
04.09.2014	Home Depot	0,010449485	-0,000291794	1,07%
05.09.2014	Home Depot	0,018681371	0,005115176	1,36%
08.09.2014	Home Depot	-0,008623416	-0,001558047	-0,71%
09.09.2014	Home Depot	-0,020810393	-0,004415209	-1,64%
10.09.2014	Home Depot	0,003598062	0,003971444	-0,04%
11.09.2014	Home Depot	-0,000336268	0,001696698	-0,20%
29.09.2014	JPMorgan Chase	-0,003797926	-0,002526822	-0,13%
30.09.2014	JPMorgan Chase	-0,001491509	-0,002792865	0,13%
01.10.2014	JPMorgan Chase	-0,007802257	-0,014433205	0,66%
02.10.2014	JPMorgan Chase	-0,008927119	0,000312379	-0,92%
03.10.2014	JPMorgan Chase	0,024813231	0,012728992	1,21%
06.10.2014	JPMorgan Chase	-0,001990403	-0,001434682	-0,06%
07.10.2014	JPMorgan Chase	-0,015121071	-0,016522033	0,14%
25.05.2011	Lockheed Martin	-0,001781524	0,003004203	-0,48%
26.05.2011	Lockheed Martin	-0,009176572	0,003467519	-1,26%
27.05.2011	Lockheed Martin	0,003507266	0,003544425	0,00%
31.05.2011	Lockheed Martin	0,008283565	0,007462903	0,08%
01.06.2011	Lockheed Martin	-0,027470839	-0,012621925	-1,48%
14.02.2020	MGM Resorts	-0,008804916	0,002771232	-1,16%
18.02.2020	MGM Resorts	0,015863091	-0,003749636	1,96%
19.02.2020	MGM Resorts	0,002186044	0,006689456	-0,45%
20.02.2020	MGM Resorts	0,007790451	-0,004975618	1,28%
21.02.2020	MGM Resorts	-0,029375381	-0,014150988	-1,52%
24.02.2020	MGM Resorts	-0,053838756	-0,04563026	-0,82%
27.11.2018	Marriott	0,000583947	0,002569061	-0,20%
28.11.2018	Marriott	0,018504498	0,023174122	-0,47%
29.11.2018	Marriott	-0,00286449	-0,003122335	0,03%
30.11.2018	Marriott	-0,055892848	0,007700449	-6,36%
03.12.2018	Marriott	0,039120179	0,010596612	2,85%

04.12.2018	Marriott	-0,050447469	-0,034671069	-1,58%
25.09.2018	Meta	-0,003022678	-0,0035351	0,05%
26.09.2018	Meta	0,012370355	-0,007019016	1,94%
27.09.2018	Meta	0,01132065	0,003608351	0,77%
28.09.2018	Meta	-0,025941726	-0,001255616	-2,47%
01.10.2018	Meta	-0,012282565	0,005149663	-1,74%
02.10.2018	Meta	-0,019145419	-0,00194008	-1,72%
03.10.2018	Meta	0,019456295	5,76536E-06	1,95%
17.01.2023	PepsiCo	0,004679212	-0,000813205	0,55%
18.01.2023	PepsiCo	-0,025218709	-0,008041539	-1,72%
19.01.2023	PepsiCo	-0,011595251	-0,003808708	-0,78%
20.01.2023	PepsiCo	0,001473626	0,010376893	-0,89%
23.01.2023	PepsiCo	-0,004473594	0,006617966	-1,11%
24.01.2023	PepsiCo	0,009283344	-0,000108652	0,94%
25.01.2023	PepsiCo	0,00726461	0,000174336	0,71%
29.05.2019	Quest Diagnostics	-0,002987082	-0,004385934	0,14%
30.05.2019	Quest Diagnostics	-0,008366634	0,002306829	-1,07%
31.05.2019	Quest Diagnostics	-0,00093752	-0,009053184	0,81%
03.06.2019	Quest Diagnostics	0,002606615	-0,001305855	0,39%
04.06.2019	Quest Diagnostics	0,010919412	0,016667728	-0,57%
05.06.2019	Quest Diagnostics	0,005554922	0,00681061	-0,13%
06.06.2019	Quest Diagnostics	0,010230019	0,005305531	0,49%
12.08.2021	T-Mobile	0,001037279	0,004152284	-0,31%
13.08.2021	T-Mobile	0,001381823	0,001801656	-0,04%
16.08.2021	T-Mobile	-0,029046662	0,002739977	-3,18%
17.08.2021	T-Mobile	-0,000426158	-0,006223025	0,58%
18.08.2021	T-Mobile	-0,005971328	-0,009637096	0,37%
19.08.2021	T-Mobile	0,00758051	0,001477064	0,61%
20.08.2021	T-Mobile	0,006530015	0,007850955	-0,13%
16.12.2013	Target	-0,003046546	0,003101359	-0,61%
17.12.2013	Target	-0,00836376	-0,003468838	-0,49%
18.12.2013	Target	0,03081892	0,010304024	2,05%

19.12.2013	Target	-0,022029914	-0,001710659	-2,03%
20.12.2013	Target	0,005470338	0,002054349	0,34%
23.12.2013	Target	-0,009761497	0,002402623	-1,22%
24.12.2013	Target	-0,002747408	0,000727215	-0,35%
15.02.2018	Tesla	0,036486631	0,013473486	2,30%
16.02.2018	Tesla	0,004250555	-0,000905465	0,52%
20.02.2018	Tesla	-0,002146044	-0,008546187	0,64%
21.02.2018	Tesla	-0,004391141	-0,008122174	0,37%
22.02.2018	Tesla	0,038613854	-0,000167708	3,88%
23.02.2018	Tesla	0,016985883	0,018341115	-0,14%
24.02.2022	Toyota	-0,008757629	0,010765309	-1,95%
25.02.2022	Toyota	0,017285723	0,015718376	0,16%
28.02.2022	Toyota	-0,013108122	-0,000855884	-1,23%
01.03.2022	Toyota	-0,006777791	-0,009559292	0,28%
02.03.2022	Toyota	-0,014088458	0,013227099	-2,73%
03.03.2022	Toyota	-0,017080561	-0,002734076	-1,43%
04.03.2022	Toyota	-0,030325508	-0,004523646	-2,58%
26.03.2018	Under Armour	0,05640053	0,038163291	1,82%
27.03.2018	Under Armour	-0,013797213	-0,02444534	1,06%
28.03.2018	Under Armour	-0,006691034	-0,004212029	-0,25%
29.03.2018	Under Armour	0,001224768	0,019299728	-1,81%
02.04.2018	Under Armour	-0,01529052	-0,031576649	1,63%
03.04.2018	Under Armour	0,044720453	0,017672495	2,70%
07.10.2020	Walgreens	0,015020817	0,015273004	-0,03%
08.10.2020	Walgreens	0,01589472	0,00545888	1,04%
09.10.2020	Walgreens	-0,019692411	0,006277968	-2,60%
12.10.2020	Walgreens	0,01623539	0,014247387	0,20%
13.10.2020	Walgreens	-0,020308597	-0,0095102	-1,08%
14.10.2020	Walgreens	-0,007462732	-0,009840824	0,24%
16.05.2014	eBay	0,011487393	0,00361737	0,79%
19.05.2014	eBay	0,007314887	0,003724436	0,36%

20.05.2014	eBay	-0,007070646	-0,007596223	0,05%
21.05.2014	eBay	-0,001539377	0,008399406	-0,99%
22.05.2014	eBay	-0,00732495	0,002101772	-0,94%
23.05.2014	eBay	0,010096947	0,004166184	0,59%
09.12.2020	SolarWinds	-0,017747647	-0,000322246	-1,74%
10.12.2020	SolarWinds	0,008616521	0,002047431	0,66%
11.12.2020	SolarWinds	0,003007453	-0,000860009	0,39%
14.12.2020	SolarWinds	-0,166912915	-0,005842716	-16,11%
15.12.2020	SolarWinds	-0,079495071	0,010350969	-8,98%
16.12.2020	SolarWinds	-0,001700006	0,001377539	-0,31%
22.06.2017	Maersk	-0,002356784	-0,004109636	0,18%
23.06.2017	Maersk	-0,00393699	-0,002259505	-0,17%
26.06.2017	Maersk	0,01897237	-0,000751965	1,97%
27.06.2017	Maersk	-0,00465463	-0,018310634	1,37%
28.06.2017	Maersk	0,018706018	-0,003587195	2,23%
29.06.2017	Maersk	-0,006886086	-0,018058282	1,12%
30.06.2017	Maersk	0,00847459	0,009188588	-0,07%
14.03.2019	Norsk Hydro	0,003186543	0,00502352	-0,18%
15.03.2019	Norsk Hydro	0,014438337	-0,003533392	1,80%
18.03.2019	Norsk Hydro	0,019926116	0,003550374	1,64%
19.03.2019	Norsk Hydro	-0,006977464	0,001675546	-0,87%
20.03.2019	Norsk Hydro	0,014052905	-0,006210492	2,03%
21.03.2019	Norsk Hydro	0,000554237	0,000873763	-0,03%
22.03.2019	Norsk Hydro	-0,033241032	-0,016086157	-1,72%
10.08.2023	Clorox Company	-0,014854784	0,000437793	-1,53%
11.08.2023	Clorox Company	0,003115474	0,000195205	0,29%
14.08.2023	Clorox Company	-0,005093371	0,00144822	-0,65%
15.08.2023	Clorox Company	-0,015983208	-0,001730424	-1,43%
16.08.2023	Clorox Company	-0,005139202	-0,00099636	-0,41%
17.08.2023	Clorox Company	-0,01677312	-0,0010253	-1,57%
18.08.2023	Clorox Company	-0,002075603	0,000364411	-0,24%