10.ETYKA DANYCH I BEZPIECZEŃSTWO INFORMACJI

Autor: Dario Šebalj

W erze transformacji cyfrowej etyczne postępowanie z danymi i ich bezpieczeństwo stały się głównymi kwestiami dla osób fizycznych i organizacji. Ponieważ codziennie gromadzone i przetwarzane są ogromne ilości danych osobowych i wrażliwych, bardzo ważne jest zapewnienie odpowiedzialnego i bezpiecznego zarządzania tymi danymi.

Niniejszy rozdział analizuje zasady etyki danych, podkreślając względy moralne i najlepsze praktyki w zakresie przetwarzania danych, a także bada różne zagrożenia dla bezpieczeństwa informacji. Rozumiejąc i zajmując się tymi kwestiami, możemy chronić prywatność, utrzymywać zaufanie i wspierać bezpieczniejsze środowisko cyfrowe.

10.1. Znaczenie etyki danych

Etyka danych odnosi się do zasad moralnych i praktyk kierujących gromadzeniem, przetwarzaniem, udostępnianiem i wykorzystywaniem danych w celu zapewnienia poszanowania praw osób fizycznych, dobrobytu społecznego i zaufania. Obejmuje przejrzystość, odpowiedzialność, uczciwość i prywatność, zapewniając, że praktyki dotyczące danych są zgodne ze standardami etycznymi i ramami prawnymi, celem zapobiegania szkodom i promowania odpowiedzialnych innowacji (Cognizant, b.d.; Gov.uk, 2020; Knight, 2021; McKinsey, 2022; Cepelak, 2023).

W dzisiejszym cyfrowym krajobrazie etyczne obchodzenie się z danymi ma kluczowe znaczenie dla utrzymania zaufania i zapewnienia przewagi konkurencyjnej. Artykuł McKinsey (2022) odnoszący się do tematu etyki danych podkreśla znaczenie włączenia kwestii etycznych do praktyk zarządzania danymi. Wskazuje na trzy powszechne błędy: zakładanie, że etyka danych jest nieistotna, poleganie wyłącznie na zespołach prawnych i zgodności w zakresie nadzoru oraz przedkładanie krótkoterminowych zysków finansowych nad praktyki etyczne. Aby rozwiązać te kwestie, zalecają kilka strategii. Po pierwsze, firmy powinny ustanowić jasne, specyficzne dla firmy wytyczne dotyczące etyki danych. Wytyczne te służą jako podstawa etycznego zarządzania danymi i pomagają w ustanowieniu standardu w całej organizacji.

Po drugie, tworzenie zróżnicowanych zespołów zajmujących się kwestiami związanymi z danymi zapewnia szeroki zakres perspektyw i zmniejsza ryzyko stronniczego podejmowania decyzji. Po trzecie, zaangażowanie kierownictwa wyższego szczebla jako mistrzów inicjatyw w zakresie etyki danych ma kluczowe znaczenie dla kierowania tymi praktykami w całej organizacji.

Rysunek 10.1. 5C Etyki Danych

Źródło: Opracowanie własne na podstawie Atlan (2023)

Rysunek 10.1 przedstawia 5C etyki danych, nakreślone przez Atlana (2023), które reprezentują podstawowe zasady etycznego postępowania z danymi:

- **Zgoda (ang. Consent):** uzyskanie świadomej, dobrowolnej zgody od osób fizycznych przed zebraniem ich danych, zapewnienie przejrzystości w zakresie wykorzystania danych.
- **Gromadzenie (ang. Collection):** gromadzenie tylko niezbędnych danych do określonych celów, unikając nadmiernego gromadzenia danych.
- **Kontrola (ang. Control):** umożliwienie osobom fizycznym dostępu do ich danych, ich przeglądania i aktualizowania, zapewniając im kontrolę nad ich wykorzystaniem.
- **Poufność (ang. Confidentiality):** ochrona danych przed nieautoryzowanym dostępem i naruszeniami dzięki solidnym środkom bezpieczeństwa.
- **Zgodność (ang. Compliance):** przestrzeganie wymogów prawnych i regulacyjnych, przeprowadzanie regularnych audytów w celu zapewnienia ciągłej zgodności.

Podobnie do zasad Atlana, Cote (2021) identyfikuje pięć podstawowych zasad etyki danych, które są niezbędne do przestrzegania przez profesjonalistów biznesowych:

- **Własność** podkreśla, że osoby fizyczne zachowują prawo własności do swoich danych osobowych. Gromadzenie danych osobowych bez wyraźnej zgody jest zarówno niezgodne z prawem, jak i nieetyczne. Firmy muszą uzyskać zgodę za pośrednictwem jasnych umów lub cyfrowych polityk prywatności, zapewniając, że użytkownicy są świadomi i zgadzają się na praktyki gromadzenia danych.
- **Przejrzystość** obejmuje jasną komunikację dotyczącą sposobu gromadzenia, przechowywania i wykorzystywania danych. Firmy muszą informować osoby fizyczne o metodach i celach gromadzenia danych. Taka przejrzystość buduje zaufanie i pozwala użytkownikom podejmować świadome decyzje dotyczące ich danych. Zwodnicze praktyki lub zatajanie informacji o wykorzystaniu danych są zarówno nieetyczne, jak i niezgodne z prawem.
- **Prywatność** koncentruje się na odpowiedzialności firm za ochronę prywatności danych osobowych. Nawet za zgodą, dane osobowe nie powinny być udostępniane publicznie bez wyraźnej zgody danej osoby. Firmy muszą wdrożyć solidne środki bezpieczeństwa w celu ochrony danych osobowych przed nieautoryzowanym dostępem lub naruszeniami.
- **Intencja** odnosi się do etycznych motywacji stojących za gromadzeniem i wykorzystywaniem danych. Dane powinny być gromadzone i wykorzystywane do celów, które są korzystne i nieszkodliwe dla jednostek lub społeczeństwa. Etyczne praktyki w zakresie danych obejmują wykorzystywanie danych w celu poprawy doświadczeń użytkowników i ulepszenia usług bez wykorzystywania lub powodowania szkód.
- **Wynik** uwzględnia szerszy wpływ wykorzystania danych na jednostki i społeczeństwo. Firmy muszą ocenić potencjalne konsekwencje swoich praktyk w zakresie danych i dążyć do uniknięcia negatywnych skutków. Zasada ta podkreśla potrzebę etycznego przewidywania i odpowiedzialności w podejmowaniu decyzji opartych na danych.

Guzman i Dyer (2020) podkreślają, że wyzwania etyczne w praktykach związanych z danymi nie są proste i często brakuje jednoznacznych rozwiązań. Stwierdzili, że istnieje rozbieżność między oczekiwaniami etycznymi online i offline. Wiele osób postrzega pewną formę wyjątkowości w przestrzeni online, gdzie tradycyjne zasady etyczne wydają się nie mieć zastosowania. Taki sposób myślenia może prowadzić do usprawiedliwiania działań online, które zostałyby uznane za nieetyczne offline. Autorzy proponują podejście etyczne, które łączy obie sfery, podkreślając, że zasady etyczne powinny pozostać spójne niezależnie od medium.

Artykuł na temat etyki danych opublikowany przez Basl i in. (2021) bada złożony proces przechodzenia od abstrakcyjnych zasad etycznych do konkretnych, możliwych do wdrożenia obietnic w kontekście dużych zbiorów danych i sztucznej inteligencji (AI). Doszli do wniosku, że dokonanie tej zmiany jest trudne i ważne, aby zagwarantować, że etyczne zachowanie nie jest tylko teoretyczne, ale także praktyczne i znaczące.

Cztery anonimowe studia przypadków opracowane przez Princeton's Center for Information Technology Policy i Center for Human Values w celu zachęcenia do dyskursu etycznego zostały opisane przez O'Reilly'ego (2018). Jedno ze studiów przypadku bada dylematy etyczne, jakie stwarza zautomatyzowana aplikacja opieki zdrowotnej zaprojektowana w celu pomocy pacjentom z cukrzycą u dorosłych przy użyciu sztucznej inteligencji. Podkreśla ono potrzebę zrównoważenia korzyści technologicznych z zasadami etycznymi, takimi jak autonomia, sprawiedliwość i odpowiedzialność. Podjęcie tych wyzwań etycznych ma kluczowe znaczenie dla odpowiedzialnej integracji sztucznej inteligencji w opiece zdrowotnej, zapewniając, że służy ona najlepszym interesom wszystkich pacjentów. Istnieje kilka kluczowych kwestii, którymi należy się zająć:

- **Paternalizm:** aplikacja ma na celu zachęcanie pacjentów do zdrowszych zachowań poprzez nakłanianie ich do dokonywania lepszych wyborów. Chociaż takie działanie może poprawić wyniki zdrowotne, rodzi to pytania etyczne dotyczące autonomii i paternalizmu. Czy etyczne jest wpływanie przez aplikację na zachowania pacjentów, czy też powinni oni mieć pełną autonomię w podejmowaniu decyzji zdrowotnych?
- **Zgoda i przejrzystość:** Aplikacja gromadzi wrażliwe dane zdrowotne w celu skutecznego działania. Zapewnienie świadomej zgody i przejrzystości w zakresie gromadzenia, wykorzystywania i udostępniania danych ma kluczowe znaczenie. Pacjenci muszą być w pełni świadomi tego, jakie dane są gromadzone, w jaki sposób będą wykorzystywane i kto będzie miał do nich dostęp.
- **Prywatność i bezpieczeństwo danych:** Obsługa wrażliwych danych medycznych wymaga rygorystycznych środków ochrony prywatności i bezpieczeństwa. Studium przypadku podkreśla potrzebę solidnych protokołów ochrony danych w celu zabezpieczenia informacji o pacjentach przed naruszeniami i nieautoryzowanym dostępem.
- **Odpowiedzialność i rozliczalność:** Ustalenie, kto jest odpowiedzialny za decyzje i działania aplikacji jest kolejnym kluczowym aspektem. Jeśli aplikacja wyda nieprawidłowe zalecenie, które negatywnie wpłynie na zdrowie pacjenta, identyfikacja

podmiotu odpowiedzialnego (deweloperów, świadczeniodawców opieki zdrowotnej lub samej aplikacji) jest złożona, ale niezbędna do pociągnięcia do odpowiedzialności.

Nowoczesne zarządzanie danymi opiera się zasadniczo na etyce danych, która gwarantuje uczciwe, przejrzyste, odpowiedzialne i szanujące prywatność praktyki w zakresie danych. Organizacje mogą wspierać odpowiedzialne innowacje, unikać pułapek prawnych i zwiększać zaufanie poprzez przestrzeganie standardów etycznych. Włączenie silnych ram etycznych do praktyk zarządzania danymi jest nie tylko najlepszą praktyką, ale także wymogiem zrównoważonego i odpowiedzialnego rozwoju, ponieważ dane stają się coraz bardziej istotne dla operacji i podejmowania decyzji.

Innym ważnym aspektem jest bezpieczeństwo informacji, ponieważ etyka danych i bezpieczeństwo informacji są ze sobą nierozerwalnie związane. Zapewnienie etycznych praktyk w zakresie danych stanowi podstawę dla solidnych środków bezpieczeństwa informacji. Ochrona danych przed nieautoryzowanym dostępem, naruszeniami i innymi zagrożeniami bezpieczeństwa nie tylko chroni prywatność i poufność, ale także podtrzymuje zasady etyczne omówione w tym rozdziale.

10.2. Podstawy bezpieczeństwa informacji

Bezpieczeństwo informacji odnosi się do kompleksowego zestawu praktyk i zasad mających na celu ochronę informacji i systemów informatycznych przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem. Zapewnia poufność, integralność i dostępność danych poprzez wdrożenie środków ochronnych, polityk i technologii. Środki te obejmują kontrolę dostępu, szyfrowanie, odzyskiwanie po awarii oraz zgodność z normami prawnymi i regulacyjnymi w celu ograniczenia ryzyka i ochrony przed potencjalnymi zagrożeniami (Fruhlinger, 2020; CISCO, b.d., NIST, b.d.).

Bezpieczeństwo informacji ma obecnie zasadnicze znaczenie dla wiarygodności i integralności organizacji w erze cyfrowej. Jego znaczenie podkreśla rosnąca zależność od danych cyfrowych i wzrost cyberzagrożeń, które narażają wrażliwe dane. Przede wszystkim bezpieczeństwo informacji chroni wrażliwe dane przed nieautoryzowanym dostępem, naruszeniami i kradzieżą. Obejmuje to dane osobowe, dane finansowe, własność intelektualną i poufną komunikację biznesową. W miarę jak cyberataki stają się coraz bardziej wyrafinowane, ryzyko naruszenia danych rośnie, potencjalnie prowadząc do poważnych strat finansowych

i utraty reputacji. Na przykład naruszenie Equifax z 2017 r. ujawniło dane osobowe 147 milionów osób, co skutkowało ugodą w wysokości do 425 milionów dolarów (Federalna Komisja Handlu, 2022). Takie incydenty podkreślają tragiczne konsekwencje nieodpowiednich środków bezpieczeństwa informacji.

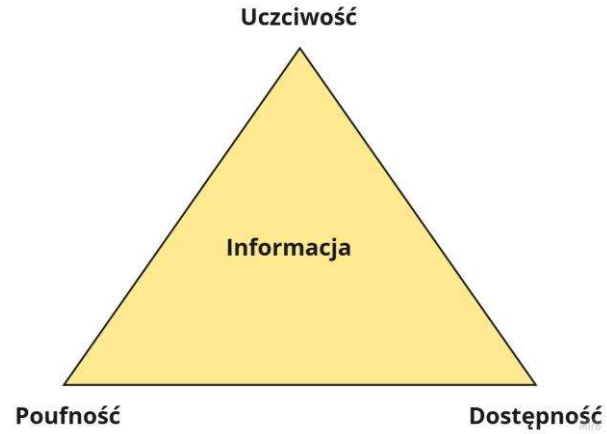
Co więcej, bezpieczeństwo informacji ma kluczowe znaczenie dla utrzymania zaufania konsumentów. W czasach, gdy prywatność danych ma kluczowe znaczenie, klienci są coraz bardziej zaniepokojeni tym, w jaki sposób przetwarzane są ich informacje. Silna architektura bezpieczeństwa informacji zapewnia, że dane konsumentów są bezpieczne, co sprzyja lojalności i zaufaniu. Według ankiety IBM, **75%** klientów nie dokonałoby zakupów w firmie, której nie ufają co do ochrony danych (PR Newswire, 2018). Bezpieczeństwo informacji jest zatem zarówno potrzebą technologiczną, jak i strategicznym imperatywem biznesowym.

Bezpieczeństwo informacji ma również kluczowe znaczenie dla łagodzenia zakłóceń operacyjnych. Cyberataki, takie jak oprogramowanie ransomware, mogą zakłócać operacje korporacyjne, uniemożliwiając użytkownikom dostęp do niezbędnych systemów do czasu zapłacenia okupu. Atak ransomware na Colonial Pipeline w 2021 r., który doprowadził do niedoborów paliwa we wschodnich Stanach Zjednoczonych, stanowi przykład destrukcyjnego potencjału takich zagrożeń (Kerner, 2022). Wdrażając silne środki bezpieczeństwa, organizacje mogą zabezpieczyć swoją ciągłość operacyjną i odporność na takie zakłócenia.

Według Kim i Solomon (2018) informacje są uważane za bezpieczne, jeśli spełniają trzy główne założenia:

- **Poufność (ang. Confidentiality):** dostęp do poufnych informacji mają tylko upoważnione osoby.
- **Uczciwość (ang. Integrity):** informacje mogą być zmieniane tylko przez osoby posiadające odpowiednie uprawnienia.
- **Dostępność (ang. Availability):** informacje i zasoby są dostępne dla autoryzowanych użytkowników zawsze, gdy są potrzebne.

Te założenia są często nazywane triadą CIA, jak pokazano na Rysunku 10.2.



Rysunek 10.2. Triada CIA

Źródło: Opracowane własne na podstawie Kim i Solomon (2018)

W bezpieczeństwie informacji pojęcia ryzyka, zagrożenia i podatności są kluczowe dla zrozumienia i zarządzania bezpieczeństwem. **Ryzyko** to prawdopodobieństwo, że coś złego stanie się z zasobem. W bezpieczeństwie informacji ryzyko to prawdopodobieństwo wystąpienia szkodliwego zdarzenia wpływającego na poufność, integralność lub dostępność informacji. Na przykład firma może ocenić ryzyko cyberataku na swoją sieć, biorąc pod uwagę zarówno prawdopodobieństwo takiego ataku, jak i potencjalne szkody, jakie może on spowodować. **Zagrożenie** to każde działanie, które może potencjalnie wyrządzić szkodę systemom informatycznym lub danym. Zagrożenia mogą być celowe, takie jak cyberataki hakerów, lub niezamierzone, takie jak klęski żywiołowe lub błędy ludzkie. **Podatność** odnosi się do słabości lub luk w zabezpieczeniach systemu, które mogą zostać wykorzystane przez zagrożenia w celu wyrządzenia szkody. Mogą to być wady oprogramowania, sprzętu, procesów organizacyjnych lub ludzkich zachowań (Kim i Solomon, 2018).

Aby skutecznie chronić systemy informatyczne, organizacje muszą zrozumieć, w jaki sposób ryzyko, zagrożenia i luki w zabezpieczeniach wzajemnie na siebie oddziałują. Na przykład luka w oprogramowaniu (np. luka w zabezpieczeniach) może zostać wykorzystana przez podmiot stanowiący zagrożenie (np. hakera), prowadząc do naruszenia danych, co stanowi ryzyko dla organizacji. Identyfikując i ograniczając luki w zabezpieczeniach, organizacje mogą zmniejszyć ryzyko wystąpienia zagrożeń powodujących znaczne szkody.

10.2.1. Naruszenie danych

Naruszenia danych stały się poważnym zagrożeniem w erze cyfrowej, wpływając na organizacje z różnych sektorów. Naruszenia te narażają na szwank poufne informacje,

prowadząc do strat finansowych, utraty reputacji i konsekwencji prawnych. Zrozumienie skali i wpływu naruszeń danych ma kluczowe znaczenie dla opracowania skutecznych strategii bezpieczeństwa w celu ochrony przed takimi incydentami. Według Fortinet (b.d.), **naruszenie danych** „to zdarzenie, które skutkuje ujawnieniem poufnych, prywatnych, chronionych lub wrażliwych informacji osobie nieupoważnionej do dostępu do nich". Naruszenia te mogą wystąpić na różne sposoby (Kaspersky, b.d.a):

1. **Przypadkowy insider (osoba mająca dostęp do poufnych informacji):** Pracownik nieumyślnie uzyskuje dostęp do poufnych informacji bez odpowiedniego upoważnienia. Na przykład, korzystając z komputera współpracownika i przeglądając poufne pliki.
2. **Złośliwy insider:** Osoba z autoryzowanym dostępem celowo nadużywa danych w szkodliwych celach. Może to obejmować kradzież lub wyciek poufnych informacji.
3. **Zgubione lub skradzione urządzenia:** Niezaszyfrowane i niezabezpieczone urządzenia, takie jak laptopy lub dyski zewnętrzne zawierające poufne dane, zostają zgubione lub skradzione, przez co informacje są narażone na nieautoryzowany dostęp.
4. **Złośliwi przestępcy zewnętrzni:** Hakerzy wykorzystują różne metody do włamywania się do systemów, w tym ataki phishingowe, ataki siłowe i złośliwe oprogramowanie. Cyberprzestępcy wykorzystują luki w oprogramowaniu, sieciach i zachowaniu użytkowników, aby uzyskać dostęp do wrażliwych danych.

Według Kaspersky (n.d.a), powszechne metody wykorzystywane w naruszeniach danych obejmują **phishing**, w którym cyberprzestępcy podszywają się pod zaufane podmioty, aby nakłonić osoby do ujawnienia poufnych informacji. Inną metodą są **ataki siłowe (brute force)**, w których hakerzy używają oprogramowania do wielokrotnego odgadywania haseł, wykorzystując słabe lub wielokrotnie używane dane uwierzytelniające w celu uzyskania nieautoryzowanego dostępu do kont. Ponadto **złośliwe oprogramowanie (malware)**, takie jak oprogramowanie szpiegujące, jest wykorzystywane do infiltracji systemów i kradzieży danych w sposób niezauważony. Metody te zostaną wyjaśnione w dalszej części rozdziału.

Błąd ludzki odpowiada za **95%** wszystkich naruszeń danych (Cybernews, 2022).

XXI wiek był świadkiem jednych z najpoważniejszych naruszeń danych, podkreślających luki w systemach cyfrowych i krytyczną potrzebę stosowania solidnych

środków bezpieczeństwa. Według Hill i Swinhoe (2022) oraz ESET (n.d.), wśród niektórych z najbardziej znaczących naruszeń danych wyróżnić można:

- **Yahoo (2013-2014):** Yahoo doświadczyło jednego z największych naruszeń danych w historii - w 2013 roku włamano się do wszystkich trzech miliardów kont użytkowników. Naruszenie to ujawniło nazwiska, adresy e-mail, daty urodzenia oraz pytania i odpowiedzi zabezpieczające. Kolejne naruszenie w 2014 r. dotknęło 500 milionów kont, jeszcze bardziej podkreślając luki w zabezpieczeniach firmy.
- **Marriott International (2018):** Marriott ogłosił, że doszło do naruszenia danych około 500 milionów gości. Hakerzy uzyskali dostęp do bazy danych rezerwacji gości Starwood, ujawniając dane osobowe, takie jak nazwiska, adresy, numery telefonów, adresy e-mail i numery paszportów. Naruszenie to było wynikiem nieautoryzowanego dostępu sięgającego 2014 roku. Biuro Komisarza ds. Informacji (ICO), brytyjski organ regulacyjny ds. danych, ostatecznie ukarał korporację grzywną w wysokości 18,4 miliona funtów w 2020 roku za brak ochrony prywatności danych osobowych swoich klientów.
- **Adult Friend Finder (2016):** Naruszenie Adult Friend Finder ujawniło dane osobowe 412 milionów kont, w tym imiona i nazwiska, adresy e-mail i hasła, z których wiele było słabo zaszyfrowanych. Incydent ten wzbudził poważne obawy dotyczące praktyk bezpieczeństwa platform internetowych obsługujących wrażliwe dane osobowe.
- **MySpace (2013):** Naruszenie danych MySpace, które miało miejsce w 2013 roku, spowodowało ujawnienie ponad 360 milionów kont użytkowników. Dane obejmowały imiona i nazwiska, adresy e-mail i hasła. Hakerzy sprzedali później te informacje w ukrytej sieci (ang. dark web), co uwypukliło luki w systemach bezpieczeństwa platform mediów społecznościowych w tym czasie.
- **LinkedIn (2021):** W 2021 roku dane osobowe 700 milionów użytkowników LinkedIn zostały opublikowane na forum dark web. Haker wykorzystał techniki screen scrapingu (wydobywania danych) za pośrednictwem interfejsu API LinkedIn w celu uzyskania adresów e-mail, numerów telefonów i innych danych osobowych. Chociaż nie był to tradycyjny atak hakerski, incydent ten wzbudził poważne obawy dotyczące prywatności danych i potencjalnego niewłaściwego wykorzystania screen scrapingu do ataków socjotechnicznych.
- **Equifax (2017):** Naruszenie to ujawniło dane osobowe prawie 148 milionów Amerykanów, 15,2 miliona Brytyjczyków i 19 000 Kanadyjczyków. Hakerzy wykorzystali

lukę we frameworku aplikacji internetowej Apache Struts, której Equifax nie zdołał załatać. Skradzione dane obejmowały numery ubezpieczenia społecznego, daty urodzenia i adresy, co doprowadziło do kosztów szacowanych na 1,7 miliarda dolarów dla Equifax.

- **eBay (2014):** eBay ujawnił naruszenie, które dotknęło 145 milionów użytkowników. Atak został przeprowadzony z wykorzystaniem naruszonych danych logowania pracowników, co doprowadziło do ujawnienia nazwisk, adresów e-mail, adresów fizycznych, numerów telefonów i zaszyfrowanych haseł. Naruszenie to uwypukliło luki w kontroli dostępu pracowników i znaczenie silnych środków uwierzytelniania.
- **Target (2013):** Naruszenie dotyczyło ponad 41 milionów kont kart płatniczych i danych kontaktowych ponad 60 milionów klientów. Cyberprzestępcy uzyskali dostęp do danych klientów, w tym nazwisk, numerów telefonów, adresów e-mail, numerów kart kredytowych i debetowych oraz zaszyfrowanych kodów PIN. Target poniósł znaczne koszty prawne i ugodowe, w tym pozew zbiorowy o wartości 10 milionów dolarów i ugodę wielostanową o wartości 18,5 miliona dolarów.

Naruszenia te pokazują daleko idące konsekwencje cyberataków i krytyczną potrzebę stosowania silnych praktyk w zakresie cyberbezpieczeństwa. Ucząc się na podstawie tych głośnych przypadków, organizacje mogą lepiej chronić swoje dane, ulepszać swoje protokoły bezpieczeństwa i minimalizować ryzyko przyszłych naruszeń. Naruszenia danych są często wynikiem szeregu podstawowych zagrożeń. Zrozumienie tych zagrożeń ma kluczowe znaczenie dla budowania skutecznych środków bezpieczeństwa informacji. Zagrożenia cybernetyczne mogą pochodzić z różnych źródeł, w tym od złośliwych intruzów, cyberprzestępców, a nawet podmiotów sponsorowanych przez państwo. Ponadto luki w systemach i sieciach mogą zostać wykorzystane do uzyskania nieautoryzowanego dostępu do poufnych informacji.

10.2.2. Zagrożenia dotyczące bezpieczeństwa informacji

Zagrożenie bezpieczeństwa to złośliwe działanie, które próbuje uszkodzić lub ukraść dane, zagrozić systemom organizacji lub całej firmie (TechTarget, 2024). Istnieje wiele różnych zagrożeń bezpieczeństwa informacji, które poważnie zagrażają dostępności, integralności i poufności danych.

Według Kim i Solomona (2018) oraz Grubba (2021) **złośliwe oprogramowanie (malware)** ma na celu infiltrację, uszkodzenie lub wyłączenie komputerów i sieci. Typowe rodzaje złośliwego oprogramowania obejmują wirusy, robaki, trojany, oprogramowanie

ransomware i oprogramowanie szpiegujące. **Wirus** to rodzaj złośliwego oprogramowania, które dołącza się do legalnego programu lub pliku i rozprzestrzenia się na inne programy i pliki po uruchomieniu zainfekowanego oprogramowania. Wirusy mogą uszkadzać lub usuwać dane, zakłócać działanie systemu i rozprzestrzeniać się na inne systemy za pośrednictwem załączników do wiadomości e-mail, połączeń sieciowych lub nośników wymiennych. W przeciwieństwie do wirusów, **robaki** są samodzielnym złośliwym oprogramowaniem, które może samoczynnie się powielać i rozprzestrzeniać niezależnie w sieciach bez konieczności dołączania do programu hosta. Robaki wykorzystują luki w systemach operacyjnych lub aplikacjach do rozprzestrzeniania się, często powodując przeciążenie sieci i przeciążenie systemów poprzez zużywanie przepustowości i zasobów. **Trojan** lub **koń trojański** to złośliwe oprogramowanie podszywające się pod legalne oprogramowanie. Użytkownicy są nakłaniani do jego instalacji, wierząc, że jest to nieszkodliwy lub przydatny program. **Ransomware** to rodzaj złośliwego oprogramowania, które szyfruje dane ofiary, czyniąc je niedostępnymi do czasu zapłacenia okupu atakującemu. Ataki ransomware mogą być niszczycielskie, prowadząc do znacznej utraty danych i zakłóceń operacyjnych, jeśli okup nie zostanie zapłacony lub kopie zapasowe nie będą dostępne. **Oprogramowanie szpiegujące** to złośliwe oprogramowanie zaprojektowane w celu gromadzenia informacji o osobie lub organizacji bez ich wiedzy Może gromadzić różne rodzaje danych, takie jak naciśnięcia klawiszy, nawyki przeglądania i dane osobowe, i przekazywać je stronom trzecim.

Innym rodzajem zagrożenia jest **phishing**. Kosinski (2024) wyjaśnia, że ataki phishingowe obejmują fałszywe wiadomości e-mail, SMS-y, połączenia telefoniczne lub strony internetowe mające na celu nakłonienie osób do ujawnienia danych osobowych lub pobrania złośliwego oprogramowania. Ataki te wykorzystują ludzkie błędy i zaufanie, dzięki czemu są bardzo skuteczne. Aby zwalczać phishing, organizacje muszą korzystać z zaawansowanych narzędzi do wykrywania zagrożeń i zapewniać solidne szkolenia pracowników, celem skutecznego rozpoznawania i reagowania na te oszustwa.

Phishing jest główną przyczyną naruszeń danych, stanowiąc 16% wszystkich naruszeń i kosztując organizacje średnio **4,76 miliona** dolarów za każde naruszenie (Kosinski, 2024).

Istnieją cztery główne rodzaje phishingu (Forbes, 2024):

- **Phishing mailowy:** wykorzystywanie poczty elektronicznej do kradzieży poufnych informacji. Atakujący mogą atakować duże grupy odbiorców, przyjmując tożsamość renomowanych organizacji.
- **Spear phishing:** wysyłanie zindywidualizowanych wiadomości e-mail, SMS-ów lub połączeń telefonicznych z zamiarem uzyskania dostępu do systemów komputerowych lub poufnych informacji. Korzystając z tej techniki, atakujący zazwyczaj wykorzystują dane z otwartych baz danych, mediów społecznościowych lub wcześniejszych naruszeń, aby wzmocnić swoją legalność.
- **Whaling:** koncentruje się na pracownikach wysokiego szczebla, w tym dyrektorach finansowych i dyrektorach naczelnych. Atakujący tworzą bardzo przekonującą, wysoce dostosowaną komunikację w celu uzyskania poufnych danych i informacji od firmy.
- **Vishing:** wykonywanie połączeń telefonicznych lub zostawianie wiadomości głosowych pod pozorem wiarygodnego źródła. Celem jest zdobycie kont bankowych, wykorzystanie danych osobowych i kradzież pieniędzy.

Zagrożenia wewnętrzne to zagrożenia bezpieczeństwa pochodzące z wewnątrz organizacji. Mogą to być pracownicy, kontrahenci lub partnerzy biznesowi, którzy mają dostęp do systemów i danych organizacji. Zagrożenia te mogą być szczególnie niebezpieczne, ponieważ insiderzy często mają legalny dostęp do poufnych informacji i systemów, co utrudnia wykrycie ich złośliwych działań (TechTarget, 2024).

Innym rodzajem zagrożenia są ataki **DDoS (Distributed Denial-of-Service)**. Ich celem jest zakłócenie normalnego ruchu docelowego serwera, usługi lub sieci poprzez przeciążenie go nadmiernym ruchem internetowym. Osiąga się to poprzez wykorzystanie wielu zainfekowanych systemów komputerowych jako źródeł ruchu atakującego. Gdy urządzenia te, często rozproszone globalnie, jednocześnie wysyłają liczne żądania do celu, zużywają dostępną przepustowość i zasoby, prowadząc do przerw w świadczeniu usług i uniemożliwiając legalnym użytkownikom dostęp do usługi (TechTarget, 2024).

Zagrożenia bezpieczeństwa w Internecie są ściśle związane z działaniami hakerów, którzy wykorzystują luki w systemach do różnych złośliwych celów. Według Grubba (2021) hakerzy są często kategoryzowani na podstawie ich intencji i metod. Dwie podstawowe kategorie to hakerzy w białych kapeluszach i hakerzy w czarnych kapeluszach. **Hakerzy w białych kapeluszach**, znani również jako etyczni hakerzy, wykorzystują swoje umiejętności do celów obronnych. Ich zadaniem jest ochrona organizacji przed cyberzagrożeniami poprzez identyfikowanie i naprawianie luk w zabezpieczeniach, zanim

złośliwi hakerzy będą mogli je wykorzystać. Z kolei **hakerzy w czarnych kapeluszach** angażują się w nielegalne działania o złych intencjach. Wykorzystują luki w zabezpieczeniach dla osobistych korzyści, które mogą obejmować kradzież danych, rozprzestrzenianie złośliwego oprogramowania lub powodowanie zakłóceń.

Jedną z kluczowych metod ochrony przed zagrożeniami bezpieczeństwa informacji jest stosowanie silnych haseł. Silne hasła, które powinny być złożone i unikalne dla każdego konta, znacznie zmniejszają ryzyko nieautoryzowanego dostępu.

Tabela 10.1 przedstawia czas potrzebny hakerowi na brutalne wymuszenie hasła, zgodnie z badaniami przeprowadzonymi przez Hive Systems (2024).

Tabela 10.1. Czas potrzebny hakerowi na złamanie hasła w 2024 r.

Liczba znaków	Tylko cyfry	Małe litery	Wielkie i małe litery	Cyfry, duże i małe litery	Cyfry, małe i wielkie litery, symbole
4	Natychmiast	Natychmiast	3 sekundy	6 sekund	9 sekund
5	Natychmiast	4 sekundy	2 minuty	6 minut	10 minut
6	Natychmiast	2 minuty	2 godziny	6 godzin	12 godzin
7	4 sekundy	50 minut	4 dni	2 tygodnie	1 miesiąc
8	37 sekund	22 godziny	8 miesięcy	3 lata	7 lat
9	6 minut	3 tygodnie	33 lat	161 lat	479 lat
10	1 godzina	2 lat	1k lat	9k lat	33k lat
11	10 godzin	44 lat	89k lat	618k lat	2m lat
12	4 dni	1k lat	4m lat	38m lat	164m lat
13	1 miesiąc	29k lat	241m lat	2bn lat	11bn lat
14	1 rok	766k lat	12bn lat	147bn lat	805bn lat
15	12 lat	19m lat	652bn lat	9tn lat	56tn lat
16	119 lat	517m lat	33tn lat	566tn lat	3qd lat
17	1k lat	13bn lat	1qd lat	35qd lat	276qd lat
18	11k lat	350bn lat	91qd lat	2qn lat	19qn lat

Źródło: Opracowanie własne na podstawie Hive Systems (2014)

Zrozumienie różnych rodzajów zagrożeń bezpieczeństwa informacji, takich jak ataki phishingowe, złośliwe oprogramowanie i ataki DDoS, podkreśla krytyczną potrzebę stosowania solidnych środków cyberbezpieczeństwa. Zagrożenia te stanowią poważne ryzyko dla danych osobowych, informacji finansowych i integralności organizacyjnej. Z tego powodu niezbędne staje się przyjęcie kompleksowych strategii bezpieczeństwa. Poniższy podrozdział przedstawia sugestie dotyczące utrzymania silnego bezpieczeństwa w Internecie, w tym praktyczne wskazówki, które ludzie i instytucje mogą wykorzystać do ochrony swoich zasobów cyfrowych.

10.2.3. Zalecenia dotyczące bezpieczeństwa informacji

Dużą liczbę zagrożeń bezpieczeństwa, takich jak phishing i złośliwe oprogramowanie, można znacznie zminimalizować, rozumiejąc je i stosując w praktyce. Istnieje kilka najważniejszych zaleceń dotyczących zapewnienia bezpieczeństwa informacji (Rubenking & Duffy, 2023; NSW Government, b.d.; Kaspersky, b.d.b):

- **Używaj silnych haseł:** twórz złożone hasła składające się z liter, cyfr i symboli dla każdego konta. Unikaj używania łatwych do odgadnięcia informacji, takich jak data urodzin. Używaj menedżera haseł do bezpiecznego przechowywania haseł i zarządzania nimi.
- Jeśli to możliwe, **włącz uwierzytelnianie wieloskładnikowe (MFA):** dodaj dodatkową warstwę zabezpieczeń, wymagając dwóch lub więcej metod weryfikacji w celu uzyskania dostępu do kont, takich jak hasło i jednorazowy kod wysłany na telefon.
- **Aktualizuj oprogramowanie:** regularnie aktualizuj systemy operacyjne, przeglądarki i aplikacje w celu załatania luk w zabezpieczeniach. W miarę możliwości włączaj automatyczne aktualizacje, aby mieć pewność, że zawsze jesteś chroniony przed najnowszymi zagrożeniami.
- **Bądź świadomy oszustw phishingowych:** nie klikaj linków ani nie pobieraj załączników z nieznanych lub podejrzanych wiadomości e-mail. Weryfikuj informacje o nadawcy i szukaj oznak phishingu, takich jak błędy ortograficzne lub pilne prośby o podanie danych osobowych.
- **Korzystaj z bezpiecznych połączeń:** upewnij się, że twoje połączenie internetowe jest bezpieczne, korzystając z wirtualnych sieci prywatnych (VPN) i unikając publicznych sieci Wi-Fi w przypadku wrażliwych działań, takich jak bankowość internetowa. Sprawdź „https://" w adresie URL, wskazujące na bezpieczne połączenie.
- **Regularne twórz kopie zapasowych danych:** regularnie twórz kopie zapasowe danych na dyskach zewnętrznych lub w chmurze. Ta praktyka zapewnia możliwość odzyskania informacji w przypadku awarii sprzętu, kradzieży lub ataku ransomware.
- **Zainstaluj oprogramowanie antywirusowe:** używaj renomowanego oprogramowania zabezpieczającego do wykrywania, zapobiegania i usuwania złośliwego oprogramowania. Aktualizuj oprogramowanie antywirusowe i wykonuj regularne skanowanie, aby upewnić się, że system jest czysty.

- **Regularne monitoruj konta:** często sprawdzaj swoje konta finansowe i internetowe pod kątem wszelkich nieautoryzowanych działań. Skonfiguruj alerty dla nietypowych transakcji i natychmiast zgłaszaj dostawcy usług wszelkie podejrzane zachowania.

Rozumiejąc etyczne implikacje przetwarzania danych i rozpoznając istniejące zagrożenia bezpieczeństwa, osoby i organizacje mogą opracować skuteczne strategie ochrony poufnych informacji. Od ustanowienia wytycznych etycznych i używania silnych, unikalnych haseł po wdrażanie zaawansowanych środków bezpieczeństwa i bycie na bieżąco z potencjalnymi zagrożeniami, praktyki te wspólnie zapewniają integralność, poufność i dostępność danych. Nadając priorytet etyce danych i solidnym protokołom bezpieczeństwa, można stworzyć bezpieczniejsze, bardziej godne zaufania środowisko cyfrowe.

BIBLIOGRAFIA

1. Atlan (2023). Data Ethics Unveiled: Principles & Frameworks Explored [dostępne: https://atlan.com/data-ethics-101/, dostęp 17.05.2024]
2. Basl, J., Sandler, R. & Tiell, S. (2021). Getting from commitment to content in AI and data ethics: Justice and explainability. Atlantic Council [dostępne: https://www.atlanticcouncil.org/in-depth-research-reports/report/specifying-normative-content/, dostęp 17.05.2024]
3. Cepelak, C. (2023). What is Data Ethics? Datacamp [dostępne: https://www.datacamp.com/blog/introduction-to-data-ethics, dostęp 14.05.2024]
4. CISCO (n.d.). What Is Information Security? [dostępne: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html, dostęp 20.05.2024]
5. Cognizant (n.d.). Data ethics [dostępne: https://www.cognizant.com/us/en/glossary/data-ethics, dostęp 14.05.2024]
6. Cote (2021). 5 Princples of Data Ethics for Business. Harvard Business School Online [dostępne: https://online.hbs.edu/blog/post/data-ethics, dostęp 17.05.2024]
7. Cybernews (2022). World Economic Forum finds that 95% of cybersecurity incidents occur due to human error [dostępne: https://cybernews.com/editorial/world-economic-forum-finds-that-95-of-cybersecurity-incidents-occur-due-to-human-error/, dostęp 21.05.2024]
8. ESET (n.d.). 5 scary data breaches that shook the world [dostępne: https://www.eset.com/in/about/newsroom/corporate-blog/corporate-blog/eset-5-scary-data-breaches-that-shook-the-world/, dostęp 21.05.2024]
9. Federal Trade Commission (2022). Equifax Data Breach Settlement [dostępne: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement, dostęp 20.05.2024]
10. Forbes (2024). Cybersecurity Stats: Facts And Figures You Should Know dostępne: https://www.forbes.com/advisor/education/it-and-tech/cybersecurity-statistics/, dostęp 24.05.2024]
11. Fortinet (n.d.). What Is A Data Breach? [dostępne: https://www.fortinet.com/resources/cyberglossary/data-breach, dostęp 21.05.2024]

12. Fruhlinger, J. (2020). What is information security? Definition, principles, and jobs. CSO [dostępne: https://www.csoonline.com/article/568841/what-is-information-security-definition-principles-and-jobs.html, dostęp 20.05.2024]
13. Gov.uk (2020). Data Ethics Framework: glossary and methodology [dostępne: https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-glossary-and-methodology, dostęp 14.05.2024]
14. Grubb, S. (2021). How Cybersecurity Really Works: A Hands-on Guide for Total Beginners. No starch press.
15. Guzman, L. & Dyer, S. (2020). Ten questions we're asking about ethics, data, and open source research. Amnesty International [dostępne: https://citizenevidence.org/2020/11/10/ethics-data-open-source/, dostęp 17.05.2024]
16. Hill, M. & Swinhoe, D. (2022). The 15 biggest data breaches of the 21st century. CSO Online [dostępne: https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html, dostęp 21.05.2024]
17. Hive Systems (2024). Are Your Passwords in the Green? [dostępne: https://www.hivesystems.com/blog/are-your-passwords-in-the-green?utm_source=tabletext, dostęp 24.05.2024]
18. Kaspersky (n.d.a). How Data Breaches Happen & How to Prevent Data Leaks [dostępne: https://www.kaspersky.com/resource-center/definitions/data-breach, dostęp 21.05.2024]
19. Kaspersky (n.d.b). Top 15 internet safety rules and what not to do online [dostępne: https://www.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online, dostęp 25.05.2024]
20. Kerner, S. M. (2022). Colonial Pipeline hack explained: Everything you need to know. TechTarget [dostępne: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know, dostęp 20.05.2024]
21. Kim, D. & Solomon, M. G. (2018). Fundamentals of Information Systems Security, 3rd Edition. Jones & Bartlett Learning.
22. Knight, M. (2021). What Is Data Ethics?. Dataversity [dostępne: https://www.dataversity.net/what-are-data-ethics/, dostęp 14.05.2024]
23. Kosinski, M. (2024). What is a phishing attack? IBM [dostępne: https://www.ibm.com/topics/phishing, dostęp 24.05.2024]

24. McKinsey (2022). Data ethics: What it means and what it takes [dostępne: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/data-ethics-what-it-means-and-what-it-takes, dostęp 14.05.2024]
25. National Institute of Standards and Technology (NIST) (n.d.). Information security [dostępne: https://csrc.nist.gov/glossary/term/information_security, dostęp 20.05.2024]
26. NSW Government (n.d.). 10 Tips for Cyber Security [dostępne: https://www.digital.nsw.gov.au/sites/default/files/2022-09/top-10-cyber-security-tips.pdf, dostęp 25.05.2024]
27. O'Reilly (2018). Case studies in data ethics [dostępne: https://www.oreilly.com/content/case-studies-in-data-ethics/, dostęp 17.05.2024]
28. PR Newswire (2018). New Survey Finds Deep Consumer Anxiety over Data Privacy and Security [dostępne: https://www.prnewswire.com/news-releases/new-survey-finds-deep-consumer-anxiety-over-data-privacy-and-security-300630067.html, dostęp 20.05.2024]
29. Rubenking, N. J. & Duffy, J. (2023). 12 Simple Things You Can Do to Be More Secure Online. PC mag [dostępne: https://www.pcmag.com/how-to/12-simple-things-you-can-do-to-be-more-secure-online, dostęp 25.05.2024]
30. TechTarget (2024). Top 10 types of information security threats for IT teams [dostępne: https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams, dostęp 24.05.2024]