

MONIKA WOŹNIAK*

Politechnika Warszawska, Warszawa, Polska

ZARZĄDZANIE BEZPIECZEŃSTWEM SIECI – IDENTYFIKACJA ZAGROŻEŃ I PRZECIWDZIAŁANIE

NETWORK SECURITY MANAGEMENT – THREAT IDENTIFICATION AND COUNTERACTING

ABSTRAKT: Organizacje w obliczu dynamicznego rozwoju Internetu i nowych technologii powinny zadbać o ochronę informacji i zasobów sieciowych, gdyż stanowią one wartość przedsiębiorstwa. Niebezpieczeństwa, zarówno te obecne w sferze wirtualnej, jak i fizycznej, stanowią zagrożenie dla funkcjonowania firmy, ze względu na możliwość spowodowania długotrwałych awarii, przerwania dostępu do świadczonych usług, a także osłabienia infrastruktury sieciowej oraz kradzieży, modyfikacji lub zmiany ważnych danych. W celu zapobiegania zaleca się stosowanie odpowiedniego oprogramowania, kontroli dostępu i szyfrowania danych. Oprócz tego ważną kwestią jest budowanie świadomości wśród pracowników na temat cyberbezpieczeństwa. Do tworzenia polityk i strategii bezpieczeństwa zaleca się korzystanie z dostępnych standardów, norm i wytycznych dotyczących bezpieczeństwa systemów i informacji, a także mapowanie ryzyka i przypisywanie im właścicieli.

SŁOWA KLUCZOWE: zarządzanie bezpieczeństwem sieci, bezpieczeństwo sieci, bezpieczeństwo informacji, zasoby sieciowe, zagrożenia.

ABSTRACT: Organizations in the face of the dynamic development of the Internet and new technologies, should take care to protect information and network resources, as they represent the value of the enterprise. Dangers, both those present in the virtual and physical spheres, pose a threat to the operation of the company, due to the possibility of causing long-term failures, interrupting access to services provided, as well as weakening the network infrastructure and stealing, modifying or altering important data. Appropriate software, access control and data encryption are recommended for prevention. In addition to this, creating awareness among employees about cyber security is an important issue. For creating security policies and strategies, it is recommended to use available standards, norms and guidelines for system and information security, as well as to map risks and assign owners to them.

KEYWORDS: network security management, network security, information security, network resources, threats.

* **Monika Woźniak**, Warsaw University of Technology, Warsaw, Poland



<https://orcid.org/0000-0002-3075-9723>



mw2013r@onet.pl

Copyright (c) 2025 Monika Woźniak. This work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License.

WPROWADZENIE

Sytuacja problemowa

Dynamika rozwoju Internetu oraz kooperujących z nim technologii, stanowi wyzwanie dla zarządzania bezpieczeństwem w sieci. W obliczu rosnącej liczby zagrożeń, zarówno dotychczas nieznanych, jak i nowych odmian znanych już niebezpieczeństw, administratorzy sieci oraz jej użytkownicy, powinni wykazywać się większą ostrożnością podczas korzystania z sieci. Aktywność w sieci, a także każde czynione w jej ramach działanie, wiąże się z transmisją danych przekazywanych między poszczególnymi elementami systemu. Podczas takiego transferu dane powinny być zabezpieczone w celu ochrony przed ich potencjalnym wyciekami lub nieuprawnionym i nieautoryzowanym dostępem.

Niemniej jednak, warto zauważyć, że to człowiek będący najniższym ogniwem sieci, jest czynnikiem decydującym czy dane niebezpieczeństwo zaistnieje, gdyż to on decyduje jakie strony internetowe odwiedza oraz jakie pliki i programy pobiera, co generuje ryzyko zainfekowania i zhakowania sieci oraz urządzeń, a w konsekwencji zamianę ryzyka wystąpienia zdarzeń niepożądanych w niebezpieczeństwo, czyli stan faktyczny. Znaczącą więc kwestią, jest budowanie świadomości wśród użytkowników w zakresie cyberhigieny, bezpieczeństwa w sieci oraz rodzajów zagrożeń i profilaktyki w zakresie bezpieczeństwa sieci.

Mimo tego, nie należy zapominać, że przyczyną ataków na sieci są też niewystarczające zabezpieczenia, nieaktualizowane oprogramowania systemów, luki w architekturze systemów, a także zastosowanie niewystarczających zasobów do zapewnienia sieci bezpiecznego funkcjonowania. Zdarza się, że systemy nie są przygotowane i odporne na każdy rodzaj ataku, stąd istotną kwestią jest monitorowanie ruchu w danej sieci oraz dbanie o jej odpowiednie zabezpieczenie.

W zakresie bezpieczeństwa sieci, znaczący więc będzie użytkownik, jaki i system, urządzenia z jakich korzysta podczas swojej działalności w sieci. Pomocne w budowaniu odpowiednich zabezpieczeń są akty prawne i regulacje, zawierające formalne definicje, a także rządowe i międzynarodowe zalecenia spisane w formie norm branżowych.

CELE BADAŃ

Cel główny i cele szczegółowe badań

Głównym celem niniejszego artykułu jest analiza zarządzania bezpieczeństwem sieci. W jego ramach wyodrębniono następujące cele szczegółowe: 1) Charakterystyka bezpieczeństwa sieci, 2) Przedstawienie zagrożeń w sieci, 3) Omówienie zarządzania bezpieczeństwem sieci w organizacji wraz ze wskazaniem narzędzi i technologii ułatwiających ten proces.

PROBLEMY BADAWCZE

Główny problem i szczegółowe problemy badawcze

Główny problem badawczy przybrał formę pytania: Na czym polega zarządzanie bezpieczeństwem w sieci? W celu rozwiązania głównego problemu badawczego sformułowano następujące szczegółowe problemy badawcze: 1) Czym jest i na czym polega bezpieczeństwo sieci? 2) Na

jakie zagrożenia może się natknąć użytkownik podczas aktywności w sieci? 3) Na czym polega zarządzanie bezpieczeństwem sieci w organizacji oraz jakie narzędzia i technologie wykorzystuje się podczas tego procesu?

HIPOTEZY BADAWCZE

Hipoteza główna i hipotezy szczegółowe

Na potrzeby artykułu, autorka przejęła następującą hipotezę główną:

Bezpieczeństwo sieci powinno być stale wzmacniane poprzez odpowiednie zarządzanie i stosowanie skutecznych narzędzi, by dostosować jego poziom do współczesnych wyzwań. W ramach tego stwierdzenia wyodrębniono trzy hipotezy szczegółowe:

1. bezpieczeństwo sieci jest procesem związanym z ochroną infrastruktury i przepływającymi za jej pośrednictwem informacjami, stąd powiązane jest z bezpieczeństwem informacji i bezpieczeństwem systemów informatycznych,
2. zarządzanie bezpieczeństwem sieci, a także stosowanie odpowiednich zabezpieczeń, zmniejsza ryzyko szkód powstałych wskutek zagrożeń związanych z obecnością i aktywnością użytkowników w sieci,
3. stosowanie odpowiednich środków ochrony zasobów organizacji takich jak zapory sieciowe, szyfrowanie danych, kontrola dostępu, cyberhigiena, polityki i strategie bezpieczeństwa, a także budowanie świadomości zagrożeń wśród pracowników, przekładają się bezpośrednio na efektywne zarządzanie bezpieczeństwem sieci.

METODY BADAWCZE

Celem uzyskania odpowiedzi na główny problem badawczy, a także składające się na niego problemy szczegółowe, zastosowane zostały metody teoretyczne, polegające na deskrypcji, analizie, wnioskowaniu przy użyciu literatury, artykułów naukowych, a także specjalistycznych internetowych witrynach.

BEZPIECZEŃSTWO W SIECI

Rozwój technologiczny sprawił, że człowiek współcześnie mierzy się z wieloma wyzwaniami. Z chwilą podłączenia urządzenia do sieci takiej jak Internet, bezpieczeństwo użytkownika związane z jego egzystencją i aktywnością w środowisku internetowym, staje się kwestią nadrzędną. Ponadto dane, którymi on dysponuje stanowią cenny towar, ponieważ ich kradzież może przynieść cyberprzestępcy wymierne korzyści finansowe, strategiczne lub operacyjne. W celu zapewnienia bezpieczeństwa użytkownika, ważne jest posiadanie odpowiednich narzędzi i oprogramowania, pozwalających na obronę przed potencjalnymi zagrożeniami. W tym celu należy dbać również o świadomość użytkowników w kwestii sieciowych niebezpieczeństw, a także edukować ich w zakresie cyberhigieny. Istotne jest, aby administratorzy sieci oraz specjaliści zajmujący się systemami informatycznymi i oprogramowaniem, regularnie monitorowali ruch sieciowy i analizowali potencjalne zagrożenia związane z atakami cybernetycznymi.

Sieć komputerowa to zbiór połączonych ze sobą komputerów połączony za pomocą medium transmisyjnego. Stanowi on system komunikacyjny, umożliwiający użytkownikom konwersacje, a także przesyłanie i wymianę między nimi informacji i zasobów. Możliwe jest to dzięki protokołom, które definiują przesył komunikatów. Sieci tworzone są przy użyciu sprzętu oraz oprogramowania i łączą urządzenia w obrębie konkretnego obszaru np. budynku biurowego¹. Sprzęt, taki jak przełącznik, router i punkt dostępu, stanowią fundament sieci komputerowych². Z perspektywy organizacji sieć komputerowa jest gwarantem korzystania ze wspólnych zasobów, gdyż niezależnie od miejsca pobytu użytkownika, zapewnia ona swobodny przepływ danych. Obecnie sieci komputerowe stanowią podstawę funkcjonowania współczesnych przedsiębiorstw.

Funkcjonowanie w sieci jest ściśle związane z zapewnieniem jej bezpieczeństwa. Jako bezpieczeństwo sieci należy rozumieć „ochronę podstawowej infrastruktury sieciowej przed nieautoryzowanym dostępem, niewłaściwym użyciem lub kradzieżą. Bezpieczeństwo to polega również na stworzeniu bezpiecznej infrastruktury dla urządzeń, aplikacji, użytkowników i aplikacji, aby mogły działać w bezpieczny sposób”³. Obejmuje ono takie elementy jak: 1) ochrona poufności danych (dane są chronione przed nieuprawnionym dostępem), 2) integralność informacji (gwarancja, że usunięcie, zniekształcenie bądź wprowadzenie zmiany w informacjach nie odbędzie się w sposób nieautoryzowany), 3) dostępność systemów (systemy powinny być dostępne dla uprawnionych do nich osób), 4) uwierzytelnienie użytkowników (proces weryfikacji tożsamości), 5) kontrola dostępu (identyfikacja użytkownika na podstawie jego danych uwierzytelniających, a następnie autoryzacji odpowiedniego poziomu dostępu po uwierzytelnieniu⁴) oraz 6) szyfrowanie transmisji (kodowanie przesyłanych danych, w taki sposób by stały się nieczytelne). Informacje stanowiące kluczowy element funkcjonowania organizacji by były bezpieczne to muszą być skutecznie zabezpieczone. Zaawansowane mechanizmy ochrony wymagają holistycznego podejścia, które integruje nowoczesne technologie, odpowiednio zaprojektowane procedury organizacyjne oraz edukację użytkowników. Kluczowym elementem jest rozwijanie świadomości i kształtowanie kultury bezpieczeństwa cyfrowego⁵.

Na potrzeby niniejszej analizy, zdefiniowany zostanie również termin jakim jest bezpieczeństwo sieci i systemów informatycznych, scharakteryzowany w art. 6 pkt 2 dyrektywy (UE) 2022/2555. Według niej „odnosi się on do odporności systemów informatycznych, przy danym poziomie zaufania, na wszelkie zdarzenia, które mogą naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług

¹ Eskom, Nowoczesne usługi sieciowe, <https://eskom.eu/blog/co-to-sa-uslugi-sieciowe-przeczytaj-artykul> (dostęp: 07.01.2025 r.).

² IBM, What is computer networking?, <https://www.ibm.com/topics/networking>, (dostęp: 07.01.2025 r.).

³ CISCO, What Is Network Security?, <https://www.cisco.com/c/en/us/products/security/what-is-network-security.html> (dostęp: 07.01.2025 r.).

⁴ Microsoft, What is access control?, <https://www.microsoft.com/pl-pl/security/business/security-101/what-is-access-control> (dostęp: 08.01.2025 r.).

⁵ nFlo, Bezpieczeństwo w sieci – Co to jest, główne zagrożenia, szyfrowanie, segmentacja sieci i polityka bezpieczeństwa, <https://nflo.pl/baza-wiedzy/bezpieczenstwo-w-sieci/>, (dostęp: 08.01.2025 r.).

oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem”⁶. Nieodłącznym więc elementem związanym z bezpieczeństwem sieci i systemów informatycznych w organizacji jest bezpieczeństwo informacji, które powinno być zapewnione przez sieć i infrastrukturę techniczną.

W kontekście wspomnianej definicji, warto przytoczyć własności bezpieczeństwa informacji, czyli tzw. triadę CIA, które są fundamentem bezpieczeństwa technologii informatycznych i ochrony danych. Należą do niej: 1) poufność (*ang. confidentiality*), 2) integralność (*ang. integrity*) i 3) dostępność (*ang. availability*). Terminy te zdefiniowano w NSC⁷ 7298, Słowniku kluczowych pojęć z zakresu cyberbezpieczeństwa, wydanym w Warszawie w 2021 r. Według niego przez poufność rozumie się „zapewnienie stosowania zatwierdzonych ograniczeń w zakresie ujawniania i dostępu do informacji, w tym środków ochrony prywatności i informacji osobistych”, jako integralność „informację, która nie uległa nieuprawnionej modyfikacji lub zniszczeniu, w tym świadczący o niezaprzeczalności i autentyczności informacji”, zaś jako dostępność „zapewnienie terminowego i niezawodnego dostępu do informacji i możliwość wykorzystania tej informacji”⁸. Pracownicy i współpracownicy firm na co dzień mają do czynienia z dużą ilością wrażliwych danych, które wytwarzają, przetwarzają, przesyłają i się nimi wymieniają. Informacje te są przesyłane drogą elektroniczną oraz magazynowane na dyskach, a także tworzone i edytowane na dyskach w chmurze. Warto wspomnieć, że każdy z pracowników ma dostęp do określonych danych, które posiadają konkretny stopień tajności. Dostęp do poszczególnych danych i przepływ informacji w organizacji powinien być monitorowany. Wykryte w ten sposób anomalie, mogą zapobiec niebezpieczeństwom lub ograniczyć straty nimi spowodowane do nieznacznych. Efektywne zarządzanie ryzykiem w obszarze bezpieczeństwa informacji, zwiększa poziom ochrony w sieci i może zabezpieczyć organizację przed utratą reputacji, stratami finansowymi czy kradzieżą danych będących informacjami poufnymi, stanowiącymi wartość przedsiębiorstwa i determinującymi jego zyski oraz pozycję na rynku.

SIEĆ JAKO ŚRODOWISKO PEŁNE ZAGROZEŃ

Sieć w obliczu dynamicznego rozwoju technologii, staje się przestrzenią pełną pułapek i niebezpieczeństw dla obecnych w niej użytkowników. Aktywność w świecie wirtualnym może być związana z kradzieżą danych i ich wyciekiem, a także z zainfekowaniem oprogramowań i sprzętów. W literaturze można się natknąć na różnego rodzaju podziały zagrożeń. Najczęściej są one klasyfikowane ze względu na czynnik wywołujący, a także lokalizację⁹. W celu niniejszej analizy,

⁶ Dziennik Urzędowy Unii Europejskiej, KOMUNIKAT KOMISJI Wytyczne Komisji dotyczące stosowania art. 4 ust. 1 i 2 dyrektywy (UE) 2022/2555 (NIS 2) (2023/C 328/02), <https://sip.lex.pl/akty-prawne/dzienniki-UE/komunikat-komisji-wytyczne-komisji-dotyczace-stosowania-art-4-ust-1-i-2-72205967>, (dostęp: 04.01.2025).

⁷ Narodowe Standardy Cyberbezpieczeństwa (NSC) to zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informacyjnych wykorzystywanych przez podmioty chcące efektywnie zarządzać systemami bezpieczeństwa informacji.

⁸ Gov.pl, Narodowe Standardy Cyberbezpieczeństwa, <https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber>, (dostęp: 04.01.2025 r.).

⁹ P. Sajler-Fudro, Zagrożenia Bezpieczeństwa w użytkowaniu systemów informatycznych – klasyfikacja i metody zapobiegania, *Nauki Ekonomiczne*, Tom 35/2022, DOI: 10.19251/ne/2022.35(11), <https://czasopisma.mazowiecka.edu.pl/index>.

wykorzystany zostanie autorski podział zaproponowany w literaturze przez dr inż. Jakuba Sytę, czyli podział cyberzagrożeń **ABCDEF** (nazwany od pierwszych liter kategorii zagrożeń). Wyróżnia on podstawowe grupy cyberzagrożeń¹⁰ mogących doprowadzić do cyberincydentów. Są to: ataki fizyczne (ang. *Attack*), awarie techniczne (ang. *Breakdown*), cyberataki (ang. *Cyberattack*), katastrofy (ang. *Disaster*), błędy (ang. *Errors*) oraz zagrożenia prawne (ang. *legal Failures*)¹¹.

Pierwsza kategoria jaką są ataki fizyczne opiera się na fizycznym i bezpośrednim zaatakowaniu celu. Może się to przejawiać z celowym wtargnięciem do pomieszczenia i zniszczeniem informacji bądź sprzętu, a także atakiem na kluczowy personel. W ramach tej kategorii wymieniony został wandalizm (niewielkie przypadkowe zniszczenia), sabotaż (celowe zniszczenie elementów infrastruktury o celu długotrwałego przerwania dostępu do usług), nadużycie (posiadanych uprawnień do osiągnięcia osobistych korzyści), atak na kluczowy personel (np. porwania, pobicia, zmuszenie ofiar do wykonania nieautoryzowanych czynności), kradzież tożsamości (podszywanie się pod inną osobę), a także oszustwo, czyli ataki socjotechniczne (wywieranie wpływu manipulowanie człowiekiem celem osiągnięcia pożądaných korzyści, np. nadanie dostępu do informacji lub jej udostępnienie osobie nieuprawnionej).

Kolejną grupą zagrożeń są awarie techniczne, rozumiane jako „skutek niewłaściwego funkcjonowania systemów, niewłaściwej konserwacji lub zużycia podzespołów”¹². Należy podkreślić, że w tej grupie znajdują się zagrożenia związane zarówno z uszkodzeniami sprzętu fizycznego, jak i oprogramowaniem. Usterki te nie są związane jedynie z samą organizacją, ale także mogą występować u jej dostawców czy partnerów biznesowych, wpływając bezpośrednio na funkcjonowanie procesów biznesowych w firmie. Ten rodzaj zagrożeń może być też zwany biznesowym, jeśli dotyczy się przerw lub braku dostaw mediów, awarii sprzętu oraz zagrożeń związanych z funkcjonowaniem firmy ze względów transportowo-technicznych (np. tych dotyczących łańcucha dostaw). Wśród tej grupy niebezpieczeństw wymienione zostały awarie takie jak błędy operacyjne oprogramowania (związane z aspektem niezawodności; chwilowe zawieszenia systemu), podatności (luki, błędy oprogramowania), awarie urządzeń, usterki u usługodawców (np. awaria współdzielonego dysku) oraz awarie funkcjonowania mediów (np. prądu, łącz internetowych).

Cyberataki to jedna z najszerszych kategorii, często utożsamiana z zapewnieniem bezpieczeństwa IT przed niepożądanymi czynnościami. Zagrożenia te obejmują zarówno widoczne, jak i niezauważalne formy szkodliwych działań¹³. W ramach cyberataków wyróżnione zostały zdarzenia

php/ne/article/view/967/854 (Dostęp: 08.01.2025).

¹⁰ Cyber-zagrożenia to potencjalne ataki cybernetyczne, mogące przyczynić się do kradzieży danych lub ich wyłudzeń, a także do uszkodzenia sprzętu i zniekształcenia danych.

¹¹ J. Syta, Metoda ABCDEF podziału cyber-zagrożeń, Analiza ryzyka jako podstawowa metoda zmniejszania niepewności w procesie podejmowania decyzji, Zarządzanie ryzykiem i zmianami w organizacji, praca zbiorowa Skrzypek E. [red], Wydawnictwo Katedra Zarządzania Jakością i Wiedzą, Lublin 2015, https://www.researchgate.net/publication/350648838_Metoda_ABCDEF_podzialu_cyber-zagrozen (Dostęp: 08.01.2025 r.).

¹² Ibidem

¹³ C. Mavani, H. K. Mistry, R. Patel, A. Goswami, The Role of Cybersecurity in Protecting Intellectual Property, International Journal on Recent and Innovation Trends in Computing and Communication, 20.02.2024, https://www.researchgate.net/publication/383204010_The_Role_of_Cybersecurity_in_Protecting_Intellectual_Property. (dostęp:09.01.2025r.)

takie jak nielegalne skopiowanie informacji (np. phishing¹⁴, keylogger¹⁵, atak MITM¹⁶), nieautoryzowane ujawnienie informacji (np. ransomware¹⁷, SQL Injection¹⁸), uniemożliwienie dostępu do kluczowych zasobów/usług (np. HTTP Flood Attack¹⁹), zatrucie danych (np. DNS Spoofing²⁰), skasowanie danych i zniszczenie systemów teleinformatycznych (np. atak typu Wiper²¹, atak fizyczny), nieautoryzowane wykorzystywanie mocy obliczeniowej (np. Cryptojacking²²), atakowanie innych celów (np. ataki DDoS²³), rozpowszechnianie nieprawdziwych informacji (np. deep fake²⁴) oraz hakywizm²⁵. W Raporcie Rocznym z działalności CERT Polska z 2023 r., do najczęściej zgłaszanych incydentów należały: 1) ataki phishingowe (41 423 zgłoszeń), 2) oszustwa komputerowe (34 304 zgłoszeń) oraz szkodliwe oprogramowania (1 650 zgłoszeń)²⁶. Według danych przedstawionych w tym raporcie, CERT Polska z roku na rok rejestruje coraz większą liczbę incydentów, która względem do roku 2022 stanowi ponad stu procentowy przyrost.

W podziale zagrożeń znajdują się również zagrożenia związane z działalnością sił natury, choć czasem ma w nich swój udział także człowiek. W ramach tej kategorii wymienia się klęski naturalne (np. pożary, powódzie, trzęsienia ziemi) oraz klęski budowlane (gwałtowne i niezamierzone zniszczenie budynku lub jego części oraz elementów konstrukcyjnych). Choć części z nich da się przewidzieć, to nie zawsze możliwe jest by im zapobiec lub zminimalizować ich skutki. Według badania wykonanego przez agencję badawczą PBS na zlecenie Polskiego Czerwonego Krzyża, ponad połowa respondentów uważa, że katastrofy naturalne stanowią większe zagrożenie niż dekadę temu²⁷. Wynika to głównie z ocieplenia klimatu, którego skutki można odczuć w postaci coraz częstszych i silniejszych klęsk naturalnych. Ten rodzaj zagrożeń wpływa na bezpieczeństwo fizyczne sprzętów, a także na ciągłość funkcjonowania firmy.

¹⁴ Phishing - polega na wyłudzeniu danych logowania użytkowników za pomocą fałszywych stron lub wiadomości e-mail.

¹⁵ Keylogger – złośliwe oprogramowanie śledzące naciśnięcia klawiatury, a następnie je rejestrujące, celem pozyskania wrażliwych danych.

¹⁶ Atak typu MITM (Man-in-the-Middle) – polega na przechwyceniu komunikacji pomiędzy użytkownikiem a systemem.

¹⁷ Ransomware – oprogramowanie blokujące dostęp do systemu komputerowego, a następnie żądające od ofiary okupu za odblokowanie do niego dostępu.

¹⁸ SQL Injection – polega na wstrzyknięciu złośliwego kodu SQL do zapytania do bazy danych.

¹⁹ HTTP Flood Attack - odmiana ataku DDoS, która poprzez wykorzystanie dużej ilości zapytań HTTP przeciąża serwer docelowy.

²⁰ DNS Spoofing – polega na modyfikowaniu danych DNS w celu przekierowania ruchu na fałszywe strony.

²¹ atak typu Wiper – złośliwe oprogramowanie kasuje dane przechowywane na dyskach.

²² Cryptojacking – polega na wykorzystaniu komputerów ofiar do nieautoryzowanego wydobywania kryptowalut.

²³ Atak DDoS (Distributed Denial of Service) - atak, którego celem jest zablokowanie dostępu do serwera lub usługi poprzez zalewanie go dużą liczbą zapytań, prowadzącą do przeciążenia serwera.

²⁴ Deepfake - to filmy lub nagrania audio manipulujące podobieństwem danej osoby, pozwalające na realistyczne fałszowanie obrazów, filmów lub nagrań dźwiękowych, które mogą wprowadzać w błąd szeroką publiczność.

²⁵ Hakywizm - to cyberdziałania łączące hakowanie z aktywizmem w celu promowania przekonań i walki z nieprawidłowościami.

²⁶ CERT Polska, Raport Roczny z działalności CERT Polska 2023, https://cert.pl/uploads/docs/Raport_CP_2023.pdf (dostęp: 09.01.2025 r.).

²⁷ Polski Czerwony Krzyż, 76% Polaków uważa katastrofy naturalne i te spowodowane przez człowieka za potencjalne zagrożenie dla siebie i swojej rodziny, 11.10.2024, <https://pck.pl/76-polakow-uwaza-katastrofy-naturalne-i-te-spowodowane-przez-czlowieka-za-potencjalne-zagrozenie-dla-siebie-i-swojej-rodziny/> (dostęp: 09.01.2025 r.).

Autor podziału cyber-zagrożeń, wyróżnił również typ zagrożeń, które nazwał błędami. Są one skutkiem przypadkowych i niezamierzonych działań, mogących mieć źródło w złych praktykach, błędnych decyzjach, a także w wyniku braku lub posiadania niewystarczającej wiedzy. W zakresie błędów wymienione zostały błędy operatorów (przypadkowe pomyłki pracowników), nieprzewidziane postępowanie użytkowników (prowadzące do niepożądanego funkcjonowania systemów informatycznych), a także błędne decyzje kierownicze (np. zaniechania prowadzące do cyberincydentu).

Ostatni rodzaj, zagrożenia prawne, związane są z zaniechaniem bądź brakiem dochowania należytej staranności w zakresie regulacji prawnych. Zaniechania specjalistów w zakresie cyberbezpieczeństwa w tej materii mogą być kosztowne i ryzykowne dla firmy. W ich obrębie zostały wskazane zagrożenia takie jak niezgodność z przepisami prawa (niedostosowanie się do wymogów prawnych związanych z bezpieczeństwem), niedotrzymanie wymagań (zobowiązania, które firma poprzez zapisy w dokumentach zobligowała się dotrzymać, np. wymagania wynikające z norm branżowych), utrata właściwości dowodowych posiadanych śladów cyfrowych (np. logów czy śladów w plikach pozostawionych po włamaniu, noszących znamiona informatyki śledczej) oraz brak zgodności z licencjami (złamanie postanowień licencyjnych oprogramowania).

W wyniku przedstawionych zagrożeń firma w zarządzaniu bezpieczeństwem w sieci powinna brać je pod uwagę, a także związane z nimi ryzyka. Należą do nich: ryzyka operacyjne (brak możliwości skorzystanie z zasobów i prowadzenia działalności spowodowane awarią lub atakiem cybernetycznym), finansowe (przestój w działalności i świadczeniu usług), wizerunkowe (problemy związane z utratą zaufania współpracowników i/lub klientów) oraz prawne (wyciek tajnych danych lub innych wrażliwych informacji)²⁸. Ważne jest by takie ryzyka monitorować, minimalizować lub zapobiegać ich potencjalnym skutkom.

ZARZĄDZANIE BEZPIECZEŃSTWEM SIECI

Wraz ze wzrostem cyberzagrożeń rośnie znaczenie bezpieczeństwa sieci. W celu zmniejszenia ryzyka związanego z bezpieczeństwem stosuje się podstawową praktykę zwaną zarządzaniem bezpieczeństwem sieci. Jej zadaniem jest ochrona fizycznych i wirtualnych urządzeń sieciowych, a także danych przez nie przepływających. Jako zarządzanie bezpieczeństwem sieci rozumie się „proces ochrony infrastruktury sieciowej poprzez stosowanie środków bezpieczeństwa, zasad i narzędzi przed zagrożeniami. Obejmuje ono zdefiniowane programowo zabezpieczenia obwodowe, które chronią zarówno urządzenia fizyczne, jak i wirtualne”²⁹. Zarządzanie bezpieczeństwem sieci spaja narzędzia bezpieczeństwa w ramach jednego rozwiązania. Stanowią one scentralizowane rozwiązanie, dzięki czemu każde urządzenie jest widoczne, a aktualizacje jak i samo zarządzanie bezpieczeństwem sieci staje się prostsze. By zarządzanie bezpieczeństwem sieci było skuteczne ważne są kooperujące jednostki w firmie takie jak liderzy biznesowi (odpowiadający za budżet, kierunek i priorytety w zakresie bezpieczeństwa sieci), administratorzy sieci

²⁸ Vectortechsolutions, Bezpieczeństwo sieci podstawą efektywnego biznesu, <https://vectortechsolutions.com/bezpieczenstwo-sieci-podstawa-efektywnego-biznesu/> (dostęp: 11.01.2025 r.).

²⁹ Nordleyer, What is network security management?, <https://nordlayer.com/learn/network-security/network-security-management/> (dostęp: 11.01.2025 r.).

(zajmujący się wdrożeniami, monitoringiem i utrzymaniem infrastruktury bezpieczeństwa sieci), specjaliści ds. bezpieczeństwa (specjalizujący się w zakresie oceny ryzyka, wdrażaniu rozwiązań zapewniających bezpieczeństwo i śledzący ruch w sieci pod kątem potencjalnych zagrożeń), pracownicy (poprzez przestrzeganie zasad bezpieczeństwa i świadomość znaczenia zagrożeń i ich wpływu na organizację), zewnętrznymi dostawcami usług (ich poziom bezpieczeństwa ma wpływ na łańcuch dostaw), a także organy rządowe i regulacyjne (opracowujące wytyczne, wymagania i zalecenia w zakresie bezpieczeństwa sieci i egzekwujący zgodność z tymi standardami)³⁰. Integralnym elementem zarządzania bezpieczeństwem sieci jest skuteczna identyfikacja wszystkich zasobów sieciowych. Ze względu na zarządzanie aktywami możemy skategoryzować zasoby jako urządzenia fizyczne (np. drukarki, komputery), aktywa wirtualne (np. zasoby w chmurze, usługi wirtualnego pulpitu), technologie pozwalające na przechowywanie danych (kopie zapasowe, nośniki pamięci) oraz oprogramowania (np. licencje oprogramowania). Każdy z nich powinien być skategoryzowany według rodzaju i wartości dla firmy. Przykładowo sprzęt fizyczny taki jak laptop będzie miał mniejszy priorytet i niższą wartość niż serwer zawierający poufne informacje³¹. Bezpieczeństwo sieci jest kluczowe dla realizacji dwóch głównych celów: po pierwsze, chodzi o ochronę informacji przed nieautoryzowanym dostępem, a po drugie, o zapewnienie ochrony danych przechowywanych na urządzeniach końcowych, takich jak komputery stacjonarne czy laptopy. By nimi efektywnie zarządzać wdraża się polityki i strategie, analizuje się ruch w sieci, bada się wskaźniki wydajności i przeprowadza testy porównawcze, wykonuje się testy reagowania na incydenty, wykonuje się oceny podatności i testy penetracyjne, a także zleca się audyty i przeglądy zewnętrzne.

Zarządzanie bezpieczeństwem sieci zazwyczaj obejmuje zadania takie jak ocena ryzyka, kontrola dostępu, monitorowanie sieci, szyfrowanie danych, zarządzanie poprawkami, reakcja na incydenty oraz zarządzanie zgodnością³². Pomocne w należyтым wypełnieniu tych czynności są narzędzia i technologie, które polepszają wydajność, automatyzują procesy bezpieczeństwa, minimalizują lub eliminują czynnik błędu ludzkiego, a także wspierają proces zarządzania bezpieczeństwem w organizacji. Efektywne podejście do ochrony sieci wymaga zastosowania różnych technologii, które z odmiennych perspektyw pomagają w zwalczaniu złośliwych ataków. W ich ramach możemy wyróżnić zapory sieciowe, systemy wykrywania i zapobiegania włamaniom, wirtualne sieci prywatne i narzędzia zdalnego dostępu, zapory aplikacji internetowych, system kontroli dostępu do sieci, antywirusy oraz narzędzia do szyfrowania danych.

Zapora sieciowa/ogniowa (ang. firewall) to zabezpieczenie sieciowe, którego zadaniem jest filtrowanie ruchu sieciowego, blokując połączenia, które mogą stanowić potencjalne zagrożenie i ryzyko. Chroni ono sieć lokalną przed nieautoryzowanym dostępem z zewnątrz oraz zapobiega

³⁰ Algosec, Network security management: Components & features, <https://www.algosec.com/solutions/network-security-management#who-owns-network-security-management-and-why-does-it-matter> (dostęp: 11.01.2025 r.).

³¹ J. Fitch, Network Security Management: 8 Steps To Improve Cybersecurity, Purplesec, 28.02.2024, <https://purplesec.us/learn/network-security-management/> (dostęp: 11.01.2025 r.).

³² Insights Desk, A Close View into Network Security Management Tips and Best Practices, 25.05.2023, <https://www.itsecuritydemand.com/insights/security/a-close-view-into-network-security-management-tips-and-best-practices/>, (dostęp: 11.01.2025 r.).

niepożądanemu udostępnianiu danych do sieci zewnętrznej, dzięki czemu zapobiega wyciekowi danych, stanowi ochronę przed atakami hakerskimi oraz złośliwym oprogramowaniem. Pełni funkcję bariery pomiędzy dwoma sieciami lub urządzeniami. W związku z ewaluacją zagrożeń, aby gwarantować skuteczniejsze działania, zmianie ulegają też firewalle. Początkowo, pierwsze „ściany bezpieczeństwa sieciowego” stanowiły pewnego rodzaju filtry pakietów danych, następnie zapory trzeciej generacji zabezpieczeń (ang. Firewall Toolkit - FWTK) były w stanie diagnozować niedozwolony ruch atakujących polegających na wykorzystywaniu poszczególnych elementów systemów stanowiących nadużycie lub będące szkodliwym działaniem dla systemu, zaś obecnie firewalle nowej generacji (ang. New Generation Firewalls – NGFW) są wyposażone w funkcje ochronne zorientowane na systemach zapobiegania włamaniom, kontroli aplikacji www oraz ochrony tożsamości³³. Klasyczny firewall operuje głównie na warstwie 3 (sieciowej) i 4 (transportowej) modelu OSI, kontrolując ruch na podstawie adresów IP i portów.

Innym stosowanym rodzajem zapory jest zaporą dedykowana dla aplikacji internetowych (ang. Web Application Firewall – WAF), której głównym celem jest „ochrona aplikacji internetowych przed różnymi rodzajami ataków sieciowych i zabezpieczenie ich przed potencjalnymi zagrożeniami”³⁴. Operuje ona na warstwie 7 modelu OSI (aplikacji). Kontroluje ona i filtruje ruch http, odbywający się pomiędzy stroną internetową a Internetem. Podczas monitorowania ruchu w sieci, opierając się na wcześniej ustalonych zasadach zaporą klasyfikuje napotkane zdarzenia na białą lub czarną listę. Pierwsza z nich zawiera elementy akceptowane przez serwer, zaś druga te identyfikowane jako niebezpieczne. Wspólne działanie tych list uzupełnia się wzajemnie, na bieżąco analizując swoje rekordy³⁵.

Z kolei systemy wykrywania i zapobiegania włamaniom (ang. Intrusion Detection System – IDS, Intrusion Prevention System – IPS) to „urządzenia sieciowe zwiększające bezpieczeństwo sieci komputerowych przez wykrywanie (IDS) lub wykrywanie i blokowanie ataków (IPS) w czasie rzeczywistym. W hierarchii zabezpieczania infrastruktury teleinformatycznej powinny one być lokowane jako kolejne – po firewallu – systemy ochrony”³⁶. IDS i IPS stanowią zgrabny zestaw systemów ochrony. W kontekście modelu OSI, IPS najczęściej jest powiązany z niższymi warstwami (warstwą: 1 – fizyczną, 2 – łącza danych i 3 – sieci), zaś IDS z o warstwami odpowiedzialnych za operacje na danych (warstwą: 4 – transportową, 5 – sesji, 6 – prezentacji, 7 – aplikacji). Gdy IDS wykryje zagrożenie i incydent naruszenia bezpieczeństwa, wysyła o nich powiadomienie, a następnie IPS podejmuje działania mające na celu powstrzymanie ataku poprzez minimalizację jego skutków lub aktywną odpowiedź na naruszenie bezpieczeństwa. W celu stworzenia

³³ Bezpieczny Internet, Co to jest firewall? Jak działa zaporą sieciowa? <https://bezpiecznyinternet.edu.pl/co-to-jest-firewall-i-jak-dziala/>, (dostęp: 11.01.2025 r.).

³⁴ Firewall, Web Application Firewall – zaporą dla aplikacji internetowych, 22.09.2023, <https://firewall.com.pl/web-application-firewall/> (dostęp: 11.01.2025 r.).

³⁵ IT Solution factor, Web Application Firewall (WAF), <https://itsf.com.pl/pojecia-itsf/web-application-firewall-waf/> (dostęp: 11.01.2025 r.).

³⁶ Marian Wrzesień, Łukasz Olejnik, Piotr Ryszawa, IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych, *Studia i Materiały Informatyki Stosowanej*, Tom 4, Nr 7, 2012 str. 16-21 <https://repozytorium.ukw.edu.pl/bitstream/handle/item/3532/Ids%20Ips%20systemy%20wykrywania%20i%20zapobiegania%20wlamaniom%20do%20sieci%20komputerowych.pdf?sequence=1&isAllowed=y>, (dostęp: 11.01.2025 r.).

skutecznego systemu ochrony wykorzystującego IDS/IPS, powinno się uwzględniać specyfikę organizacji, źródło i charakter przewidywanych zagrożeń, tak by przyjęte rozwiązanie było dostosowane do potrzeb firmy i stanowiło efektywny element zarządzania jej bezpieczeństwem.

W celu zapewnienia bezpiecznego połączenia z siecią firmową, organizacje stosują wirtualne sieci prywatne (ang. Virtual Private Network – VPN). Technologia ta jest przydatna szczególnie w przypadku, gdy pracownik pracuje zdalnie lub przebywa w podróży służbowej. W pierwszej kolejności użytkownik łączy się z Internetem, a następnie zabezpiecza to połączenie poprzez użycie VPN, która przekierowuje ruch w sieci przez zdalny serwer, szyfrując go w trakcie transferu. Bezpieczeństwo połączenia zależy od protokołu VPN, który jest zbiorem zasad określających sposób komunikacji między dwoma urządzeniami. Warstwa sieciowa i warstwa transportowa modelu OSI są najczęściej używane w implementacjach VPN. Wirtualne sieci prywatne są atrakcyjnym narzędziem ze względu na zapewnienie bezpieczeństwa i zwiększenie prywatności³⁷.

Ważną rolę w zarządzaniu bezpieczeństwem sieci pełni także system zdalnego dostępu, czyli narzędzia i aplikacje umożliwiające uzyskanie dostępu i kontroli do jednego komputera przy pomocy drugiego komputera podłączonego do Internetu lub tej samej sieci lokalnej. Takiego rodzaju narzędzia lub programy działają poprzez utworzenie bezpiecznego połączenia między systemami lokalnymi a zdalnymi, używając do tego szyfrowania celem zapewniania prywatności i ochrony danych³⁸. Do najczęściej używanych warstw OSI należy przede wszystkim warstwa aplikacji, a także warstwa sieciowa i transportowa. System zdalnego pulpitu często używany jest przez pracowników pomocy technicznej, w celu rozwiązania usterki poprzez wirtualne połączenie, wykluczając potrzebę fizycznej wizyty u pracownika, zgłaszającego problem natury technicznej. Oprócz tego system zdalnego dostępu jest świetnym rozwiązaniem podczas pracy zdalnej, gdyż pracownik może bezproblemowo połączyć się z urządzeniem znajdującym się w biurze i pobrać z niego ważne dokumenty³⁹.

W obliczu zagrożeń, istotną kwestią pozostaje kontrola dostępu do sieci (ang. Network Access Control - NAC). Jest to zestaw technologii i polityk umożliwiający administrowanie siecią poprzez określenie urządzeń i pracowników, którzy powinni mieć dostęp do określonych zasobów sieciowych. System ten odpowiada za weryfikację, czy dane urządzenie może połączyć się z siecią. W odpowiedzi na wysłane żądanie, urządzenia otrzymują dostęp lub odmowę dostępu do sieci. NAC może działać na różnych poziomach, zarówno fizycznym, jak i w warstwie sieciowej lub aplikacji. Wdrożenie tego rodzaju systemu zapewnia szereg kwestii związanych z bezpieczeństwem,

³⁷ M. Woźniak, Wirtualne sieci prywatne – charakterystyka i bezpieczeństwo, Wiedza Obronna 2024, Tom 289 Nr 4/2024, DOI: <https://doi.org/10.34752/2024-4-1>, <https://wiedzaobronna.edu.pl/index.php/wo/article/view/303/306>, (dostęp: 11.01.2025 r.).

³⁸ TSplus, Co to jest oprogramowanie do zdalnego dostępu?, <https://tsplus.net/pl/remote-access/blog/what-is-remote-access-software/>, (dostęp: 11.01.2025 r.).

³⁹ IT solution factor, Systemy zdalnego dostępu, <https://itsf.com.pl/pojecia-itsf/systemy-zdalnego-dostepu/>, (dostęp: 11.01.2025 r.).

takich jak ochrona przed złośliwym oprogramowaniem, kontrola urządzeń i dostępu, monitorowanie sieci czy wdrażanie zasad bezpieczeństwa⁴⁰.

Antywirusy są jednym z podstawowych mechanizmów ochrony przed zagrożeniami, gdyż chronią systemy komputerowe przed zainfekowaniem. Są one rodzajami oprogramowania, których zadaniem jest „wykrywanie, neutralizowanie i usuwanie wirusów komputerowych oraz innych złośliwych programów, takich jak trojany, robaki, spyware czy adware”⁴¹. Oprogramowanie antywirusowe działa na różnych poziomach modelu OSI, ale główna warstwa, na której operuje, to warstwa aplikacji. Podczas gdy użytkownik korzysta z urządzenia, programy te działają w tle. Skanują one wówczas pliki, programy oraz aktywność w sieci w celu wykrycia potencjalnego zagrożenia. W momencie wykrycia zagrożenia, antywirus podejmuje działania mające na celu jego izolację lub usunięcie⁴². Oprogramowanie to zwiększa ochronę przed niebezpieczeństwami i minimalizuje ryzyko ataku cybernetycznego.

Obecnie ciężko jest wyobrazić sobie by ważne i cenne dane nie zostały zabezpieczone podczas ich transferu do miejsca docelowego. Szyfrowanie danych polega na przekształceniu danych, w taki sposób by pozostały one nieczytelne dla osób do nich nieuprawnionych. Proces szyfrowania danych odbywa się za pomocą klucza kryptograficznego, który stanowi określony zbiór wartości liczbowych znanych nadawcy i odbiorcy komunikatu. Odszyfrowanie komunikatu jest możliwe dla każdej osoby posiadającej odpowiedni dla danego szyfru klucz. Skuteczne szyfrowanie wykorzystuje klucze o wysokim stopniu złożoności, przez co pozostają bardzo trudne do złamania⁴³. Najczęściej używane warstwy modelu OSI dla szyfrowania to warstwa aplikacji, transportowa, sieciowa oraz łącza danych. Szyfrowanie danych gwarantuje prywatność, integralność oraz bezpieczeństwo.

W celu skutecznego zarządzania bezpieczeństwem sieci, oprócz narzędzi i technologii istotne jest wdrażanie określonych procedur i polityk bezpieczeństwa, a także budowanie świadomości na temat bezpieczeństwa sieci i cyberhigieny wśród pracowników. W tym procesie tworzenia strategii niezwykle pomocne dla organizacji są ramy i zasady bezpieczeństwa. Wśród tych najbardziej znanych można wyróżnić Ramy cyberbezpieczeństwa NIST i powstałe na ich wzór polskie Narodowe Standardy Cyberbezpieczeństwa, kontrole bezpieczeństwa CIS, Framework MITRE ATT&CK, a także korzystanie z zasady Zero Trust („nigdy nie ufaj, zawsze weryfikuj”)⁴⁴.

⁴⁰ Polityka bezpieczeństwa, Co to jest Network Access Control - NAC?, <https://www.politykabezpieczenstwa.pl/pl/a/co-to-jest-network-access-control-nac>, (dostęp: 11.01.2025 r.).

⁴¹ Nflo, Co to jest Antywirus?, <https://nflo.pl/slownik/antywirus/> (dostęp: 11.01.2025 r.).

⁴² WAT, Oprogramowanie antywirusowe – niezbędny element ochrony Twojego komputera, 29.08.2023, <https://promocja.wat.edu.pl/cyberwat/oprogramowanie-antywirusowe-niezbedny-element-ochrony-twojego-komputera/>, (dostęp: 11.01.2025 r.).

⁴³ Kingston, Co to jest szyfrowanie i jak działa?, <https://www.kingston.com/pl/blog/data-security/what-is-encryption>, (dostęp: 11.01.2025 r.).

⁴⁴ LevelBlue, What is network security? Network security technologies explained, <https://levelblue.com/blogs/security-essentials/network-security-and-technologies-explained>, (dostęp: 11.01.2025 r.).

PODSUMOWANIE

Zarządzanie bezpieczeństwem sieci to bardzo ważny proces, zapewniający poprawne funkcjonowanie organizacji. Polega on na ochronie podstawowej infrastruktury sieciowej przed zagrożeniami. Kluczowym elementem dla zapewnienia bezpieczeństwa sieci i systemów informatycznych w organizacji jest bezpieczeństwo informacji. Jego głównymi celem jest zapewnienie poufności, integralności i dostępności przesyłanych informacji, czyli tzw. triady CIA. Oprócz tego ważne jest, by zapewnić dostęp do odpowiednich informacji osobom do nich uprawnionym, posiadającym odpowiedni dostęp do tajności danych. Niezbędna do prawidłowego przebiegu tego procesu jest kontrola danych, zawierająca takie elementy jak weryfikacja, autoryzacja i uwierzytelnianie.

Każda organizacja powinna klasyfikować swoje aktywa, według priorytetu i wartości, w ten sposób zapewniając skuteczną identyfikację posiadanych zasobów sieciowych. Znając je organizacja jest w stanie dobrać odpowiednie środki ochrony przed potencjalnymi niebezpieczeństwami takimi jak kradzież sprzętu, włamanie do systemu, a także zmiana i zniszczenie danych.

Szacując potencjalne zagrożenia i mając świadomość ich skutków, a także uwzględniając specyfikę firmy, możliwe jest dobranie takich metod i środków walki z niebezpieczeństwami, by w odniesieniu do konkretnej organizacji były one jak najbardziej skuteczne. Oczywiście należy uwzględniać też ryzyka związane z wystąpieniem tych niebezpieczeństw. Skuteczne zarządzanie bezpieczeństwem sieci wymaga nie tylko odpowiednich narzędzi i technologii, ale także wdrożenia właściwych procedur oraz polityk bezpieczeństwa. Istotnym elementem jest również edukowanie pracowników w zakresie bezpieczeństwa sieciowego i przestrzegania zasad cyberhigieny.

BIBLIOGRAFIA

REFERENCES LIST

PIŚMIENICTWO

LITERATURE

Ćwik B., *Postrzeganie zagrożeń w systemach bezpieczeństwa organizacji*, Modern Management Review, 2018, https://www.researchgate.net/publication/323105727_POSTRZEGANIE_ZAGROZEN_W_SYSTEMACH_BEZPIECZENSTWA_ORGANIZACJI.

Fidelis O. F., Lawrence A. S., *AN OVERVIEW OF NETWORK SECURITY AND MANAGEMENT*, 2024, https://www.researchgate.net/publication/381480940_AN_OVERVIEW_OF_NETWORK_SECURITY_AND_MANAGEMENT.

J. Syta, *Metoda ABCDEF podziału cyber-zagrożeń, Analiza ryzyka jako podstawowa metoda zmniejszania niepewności w procesie podejmowania decyzji, Zarządzanie ryzykiem i zmianami w organizacji*, praca zbiorowa Skrzypek E. [red], Wydawnictwo Katedra Zarządzania Jakością i Wiedzą, Lublin 2015, https://www.researchgate.net/publication/350648838_Metoda_ABCDEF_podzialu_cyber-zagrozen.

Mavani C., Mistry H. K., Patel R., Goswami A., *The Role of Cybersecurity in Protecting Intellectual Property, International Journal on Recent and Innovation Trends in Computing and Communication*, 20.02.2024, https://www.researchgate.net/publication/383204010_The_Role_of_Cybersecurity_in_Protecting_Intellectual_Property.

Mencel A., *Identyfikacja zagrożeń wynikających z użytkowania systemów informatycznych*, Akademicki Przegląd Biznesu i ekonomii, Vol. 2(1) · 2022.

Sajler-Fudro P., *Zagrożenia bezpieczeństwa w użytkowaniu systemów informatycznych – klasyfikacja i metody zapobiegania*, Nauki Ekonomiczne, Tom 35/2022, DOI: 10.19251/ne/2022.35(11), <https://czasopisma.mazowiecka.edu.pl/index.php/ne/article/view/967/854>.

Woźniak M., *Wirtualne sieci prywatne – charakterystyka i bezpieczeństwo*, Wiedza Obronna 2024, Tom 289 Nr 4/2024, DOI: <https://doi.org/10.34752/2024-4-1>, <https://wiedzaobronna.edu.pl/index.php/wo/article/view/303/306>.

Wrzesień M., Olejnik Ł., Ryszawa P., *IDS/IPS: Systemy wykrywania i zapobiegania włamaniom do sieci komputerowych*, Studia i Materiały Informatyki Stosowanej, Tom 4, Nr 7, 2012 str. 16-21, <https://repozytorium.ukw.edu.pl/bitstream/handle/item/3532/Ids%20Ips%20systemy%20wykrywania%20i%20zapobiegania%20wlamaniom%20do%20sieci%20komputerowych.pdf?sequence=1&isAllowed=>.

ŹRÓDŁA

SOURCES

Algosec, *Network security management: Components & features*, <https://www.algosec.com/solutions/network-security-management#who-owns-network-security-management-and-why-does-it-matter>.

Bezpiecznyinternet, *Co to jest firewall? Jak działa zaporą sieciową?*, <https://bezpiecznyinternet.edu.pl/co-to-jest-firewall-i-jak-dziala/>.

CERT Polska, *Raport Roczny z działalności CERT Polska 2023*, https://cert.pl/uploads/docs/Raport_CP_2023.pdf.

CISCO, *What Is Network Security?*, <https://www.cisco.com/c/en/us/products/security/what-is-network-security.html>.

Dziennik Urzędowy Unii Europejskiej, Komunikat Komisji Wytyczne Komisji dotyczące stosowania art. 4 ust. 1 i 2 dyrektywy (UE) 2022/2555 (NIS 2) (2023/C 328/02).

Eskom, *Nowoczesne usługi sieciowe*, <https://eskom.eu/blog/co-to-sa-uslugi-sieciowe-przeczytaj-artykul>.

Firewall, *Web Application Firewall – zaporą dla aplikacji internetowych*, 22.09.2023, <https://firewall.com.pl/web-application-firewall/>.

Gov.pl, *Narodowe Standardy Cyberbezpieczeństwa*, <https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber>.

IBM, *What is computer networking?*, <https://www.ibm.com/topics/networking>.

Insights Desk, *A Close View into Network Security Management Tips and Best Practices*, 25.05.2023, <https://www.itsecuritydemand.com/insights/security/a-close-view-into-network-security-management-tips-and-best-practices/>.

IT solution factor, *Systemy zdalnego dostępu*, <https://itsf.com.pl/pojecia-itsf/systemy-zdalnego-dostepu/>,

IT Solution factor, *Web Application Firewall (WAF)*, <https://itsf.com.pl/pojecia-itsf/web-application-firewall-waf/>.

J. Fitch, Purplesec, *Network Security Management: 8 Steps To Improve Cybersecurity*, 28.02.2024, <https://purplesec.us/learn/network-security-management/>.

Kingston, *Co to jest szyfrowanie i jak działa?*, <https://www.kingston.com/pl/blog/data-security/what-is-encryption>.

LevelBlue, *What is network security? Network security technologies explained*, <https://levelblue.com/blogs/security-essentials/network-security-and-technologies-explained>.

Microsoft, *What is access control?*, <https://www.microsoft.com/pl-pl/security/business/security-101/what-is-access-control>.

nFlo, *Bezpieczeństwo w sieci – Co to jest, główne zagrożenia, szyfrowanie, segmentacja sieci i polityka bezpieczeństwa*, <https://nflo.pl/baza-wiedzy/bezpieczenstwo-w-sieci/>.

Nflo, *Co to jest Antywirus?*, <https://nflo.pl/slownik/antywirus/>.

Nordleyer, *What is network security management?*, <https://nordlayer.com/learn/network-security/network-security-management/>.

Polityka bezpieczeństwa, *Co to jest Network Access Control - NAC?*, <https://www.politykabezpieczenstwa.pl/a/co-to-jest-network-access-control-nac>.

Polski Czerwony Krzyż, *76% Polaków uważa katastrofy naturalne i te spowodowane przez człowieka za potencjalne zagrożenie dla siebie i swojej rodziny*, 11.10.2024, <https://pck.pl/76-polakow-uwaza-katastrofy-naturalne-i-te-spowodowane-przez-czlowieka-za-potencjalne-zagrozenie-dla-siebie-i-swojej-rodziny/>.

TSplus, *Co to jest oprogramowanie do zdalnego dostępu?* <https://tsplus.net/pl/remote-access/blog/what-is-remote-access-software/>.

Vectortechsolutions, *Bezpieczeństwo sieci podstawą efektywnego biznesu*, <https://vectortechsolutions.com/bezpieczenstwo-sieci-podstawa-efektywnego-biznesu/>.

WAT, *Oprogramowanie antywirusowe – niezbędny element ochrony Twojego komputera*, 29.08.2023, <https://promocja.wat.edu.pl/cyberwat/oprogramowanie-antywirusowe-niezbedny-element-ochrony-twojego-komputera/>.

OPEN  ACCESS

Copyright (c) 2025 Monika Woźniak.



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License