METODY OCHRONY PRZED CYBERPRZESTĘPCZOŚCIĄ

METHODS FOR PROTECTION AGAINST CYBERCRIME

Władysław Wornalkiewicz

Wladyslaw Wornalkiewicz

Abstrakt

Coraz częściej środki masowego przekazu informują nas o zaistniałych zagrożeniach, jakie wystąpiły w eksploatowanych konfiguracjach sieci komputerowych obiektów oraz w zakresie uszkodzeń systemów, spowodowanych atakiem cyberprzestępców do zasobów informacji. W tym opracowaniu podjęto się wprowadzenia do problematyki ochrony sieci teleinformatycznych i baz danych przed zagrożeniami z cyberprzestrzeni. W tym względzie stosowane są różne rozwiązania techniki IT dla uniemożliwienia dostępu niepowołanych osób do zgromadzonych danych, a w szczególności w zakresie dotyczącym infrastruktury krytycznej, czy też informacji niejawnych. Zwrócono uwagę na dostępną w tym zakresie literaturę, akty prawne regulujące konieczność ochrony sieci i zasobów informatycznych. Podkreślono znaczenie okresowego audytu sprawdzenia podatności eksploatowanego sprzętu i aplikacji na ingerencję zewnętrzną cyberprzestępców, zwanych hakerami. Wskazano, że często pospieszne projektowanie i kodowanie funkcjonalnych systemów użytkowych wytwarza luki – możliwości wejścia ze złośliwym oprogramowaniem zwanym malware. Zamieszczone informacje należy traktować jako materiał wstępny do głębszego poznania zagadnienia ochrony sieci telekomunikacyjnych i zapobiegania cyberzagrożeniom użytkowanych systemów.

Annotation

Increasingly, the mass media inform us about the threats that occurred in the operated configurations of computer networks of objects and in the scope of damage to systems caused by the attack of cybercriminals on information resources. In this study, an introduction to the issue of protection of ICT networks and databases against threats from cyberspace was undertaken. In this regard, various IT solutions are used to prevent unauthorized persons from accessing the collected data, in the field of critical infrastructure or classified information. Attention was paid to the available literature in this area, legal acts regulating the need to protect networks and IT resources. The importance of a periodic audit to check the susceptibility of the equipment and applications used to the external interference of cybercriminals, called hackers, was emphasized. It has been pointed out that often the hasty design and coding of functional user systems creates gaps – opportunities to enter with malware. The information provided should be treated as a preliminary material for a deeper understanding of the issue of protecting telecommunications networks and preventing cyber threats to the systems used.

Słowa kluczowe: zasoby informacji, ochrona, cyberprzestępczość.

Key words: information resources, protection, cybercrime.

Wstęp

Najbardziej rozpowszechnione określenia, często używane w odniesieniu do zagadnień bezpieczeństwa teleinformatycznego wykorzystywane wymiennie to bezpieczeństwo informacyjne (*information security*) i cyberbezpieczeństwo (*cybersecurity*). Identyfikacja zagrożeń jest skomplikowanym wyzwaniem, towarzyszącym analizie problemów teleinformatycznych. Niektóre polegają na groźbie zniszczenia materialnych narzędzi służących do przechowywania, przetwarzania lub przesyłania cyfrowej informacji. Tego rodzaju niebezpieczeństwo może też być spowodowane klęskami żywiołowymi lub katastrofami technicznymi. Większość z zagrożeń bezpieczeństwa teleinformatycznego wiąże się jednak z działaniami prowadzonymi w cyberprzestrzeni, przy wykorzystaniu odpowiedniego sprzętu i oprogramowania. Wówczas negatywnemu oddziaływaniu poddawana jest sama informacja utrwalona w formie elektronicznej, a nie urządzenia służące do jej przechowywania i przetwarzania.

Wieloaspektowość i wielopłaszczyznowość zagadnienia *bezpieczeństwo teleinformatyczne* wynika z różnorodności i dużej liczby poziomów, na których należy je rozpatrywać. Może się ono bowiem odnosić użytkowników indywidualnych, przedsiębiorstw i instytucji, wykorzystujące w swej codziennej działalności całe sieci teleinformatyczne, aż po państwo, o rozległych sieciach spinających jego struktury. Złożoność problematyki bezpieczeństwa informatycznego utrudnia znalezienie cech wspólnych wszystkim zagadnieniom uznawanym za przynależne do tej dziedziny. Mimo to można przyjąć, że *istotą bezpieczeństwa teleinformatycznego jest zdolność określonego podmiotu do pozyskania i zachowania, w formie niezmienionej bez jego zgody i wiedzy, wszelkiego rodzaju informacji utrwalonej w postaci cyfrowej oraz możliwość jej bezpiecznego przetwarzania, przesyłania i upowszechniania*. Bezpieczeństwo danych przechowywanych lub przesyłanych przez poszczególne jednostki z wykorzystaniem ich własnego sprzętu uzależnione jest od poziomu odporności na rozmaite groźby infrastruktury teleinformatycznej na szczeblu narodowym. Złośliwe ataki z cyberprzestrzeni stanowią jednak coraz częściej zagrożenie dla niezawodności eksploatowanych sieci teleinformatycznych, pakietów oprogramowania oraz komunikatorów umożliwiających spotkania, naukę online i pracę zdalną.

W opracowaniu niniejszym, traktowanym jako materiał pomocniczy do specjalizacji w zakresie cyberbezpieczeństwa na kierunku *Zarządzanie*, zabazowano przede wszystkim na publikacji internetowej firmy Network Expert (wg: *https://networkexpert.pl/cyberbezpieczenstwo/*) oraz informacjach z encyklopedii Wikipedia. Bezpieczny system teleinformatyczny powinien być rozwiązaniem, które poprawnie i w całości realizuje tylko i wyłącznie cele zgodne z intencjami użytkownika (wg: *https://pl.wikipedia.org/wiki/Bezpiecze%C5%84stwo_teleinformatyczne*). W praktyce jednak budowa skomplikowanego systemu teleinformatycznego spełniającego te intencje jest z reguły niemożliwa i dlatego zapewnianie bezpieczeństwa sprowadza się do kompleksowego zarządzania ryzykiem.

Opracowano już różne systemy informatyczne chroniące sieci i zasoby informacji przed zagrożeniem z cyberprzestrzeni. Przykładowo zarządzanie dostępem do sieci teleinformatycznej obiektu może odbywać się z zastosowaniem systemu *Cisco ISE*, który jest zaawansowanym systemem zarządzania dostępem. Stosowany tu serwer *Network Admision Control* (NAC) to urządzenie, który wspiera sprzęt sieciowy w udzielaniu dostępu do danej sieci, czyli dokonuje uwierzytelniania. Ten centralny serwer może być powiązany z bazą danych użytkowników i możemy na takim serwerze tworzyć procedury dostępu do sieci. Dodam jeszcze, że system ten ma bardzo dogodny interfejs systemu GUI, co pozwala wykonywać oraz wiele operacji dostępowych do sieci.

Odniesienia literaturowe dotyczące ochrony przed cyberatakami

Cyberterroryzm oraz pokrewne mu formy wykorzystania technologii informatycznych przez podmioty pozapaństwowe stanowią działalności hakerów (wg: *https://pl.wikipedia.org/wiki/Bezpiec*

ze%C5%84stwo_teleinformatyczne). Istotne jest zatem przybliżenie zarówno metody, jak i narzędzia kodowania danych, a także sposobów i środków przełamywania tego rodzaju zabezpieczeń. Cenna jest także znajomość podmiotów zainteresowanych szyfrowaniem i odszyfrowywaniem informacji przechowywanych lub przesyłanych z wykorzystaniem technologii informatycznych oraz ocena poziomu współcześnie stosowanych przez państwa zabezpieczeń danych w formie elektronicznej. W publikacji pod linkiem (*https://www.pism.pl/publikacje/bezpieczenstwo-teleinformatyczne-panstwa*) podjęto temat wykorzystania technologii informatycznych przez struktury administracji rządowej oraz tempo rozwoju i charakteru współpracy w tej sferze w ramach Unii Europejskiej. Omówiono też proces budowy w Polsce tzw. *e-governmentu*, a więc wdrażania rozwiązań opartych na technologiach informatycznych do praktyki działania polskiej administracji publicznej, patrząc na to zagadnienie przez pryzmat inicjatyw proponowanych i zalecanych przez UE.

Zaprezentowano organy i instytucje odpowiedzialne w Unii Europejskiej za tego rodzaju zadania oraz omówiono dokonania w tym względzie w postaci rozmaitych ukończonych lub wciąż prowadzonych projektów. Wskazano na najpoważniejsze słabości, niedociągnięcia i braki tego aspektu unijnej współpracy. W cytowanej w wymienionym źródle internetowym monografii podjęto się analizy prawno-międzynarodowej dokumentu dotyczącego kwestii bezpieczeństwa teleinformatycznego, czyli *Konwencji o cyberprzestępczości* opracowanej pod auspicjami Rady Europy.

Sięgnijmy teraz po kolejną publikację „*Cyberprzestepczość*" pod linkiem: *https://www.ksiegarnia.beck.pl/10271-cyberprzestepczosc-maciej-siwicki* [2]. Wprowadza nas ona w problematykę najnowszych trendów dotyczących zagrożeń płynących z Sieci i systemów komputerowych. Stanowi jednak rodzaj wiedzy specjalistycznej, niedostępnej i często niezrozumiałej dla dużej części społeczeństwa.

Niska jest jeszcze świadomość wśród podmiotów stosujących prawo oraz użytkowników Sieci na temat natury cyberprzestępczości. Powoduje to nie zgłaszanie przez pokrzywdzonych zaistniałej sytuacji, a w rezultacie nie angażowanie Policji w ściganie oraz wykrywanie sprawców cyberataków na zasoby informatyczne. W rezultacie przestępczość zorganizowana skupiona wokół tzw. *podziemia komputerowego* przynosi znaczne zyski przy niewielkim ryzyku pociągnięcia do odpowiedzialności karnej. Przeciwdziałanie tej przestępczości wymaga jednak nie tylko zwiększenia świadomości użytkowników oraz organów ścigania i karania o zagrożeniach i kosztach powodowanych cyberprzestępczością, ale również ciągłego dostosowywania prawa do dynamicznie zmieniającej się w tym zakresie rzeczywistości. W cytowanym opracowaniu ocena zakresu i sposobu kryminalizacji cyberprzestępstw dokonana została z uwzględnieniem wypracowanych na gruncie prawa karnego wybranych państw instrumentów prawnych, na tle prawa unijnego oraz wybranych dokumentów międzynarodowych, w tym w szczególności: konwencji Rady Europy o cyberprzestępczości, *Prawa Modelowego Wspólnot Narodów* dotyczącego przestępstw komputerowych i przestępstw związanych z komputerami, przygotowanego przez Międzynarodowy Związek Telekomunikacyjny opracowania pt. „*ITU Cybercrime Legislation Toolkit*".

Zachęceni zawartością merytoryczną wcześniej wymienionych publikacji skorzystajmy z kolejnej pracy „*Cyberprzestępczość Jak walczyć z łamaniem prawa w Sieci*" [3] (wg: *https://helion.pl/ksiazki/cyberprzestepczosc-jak-walczyc-z-lamaniem-prawa-w-sieci-debra-littlejohn-shinder-ed-tittel-technica,cyber.htm#format/d)*. Wertując dalsze strony internetowe spotykamy informację o publikacji „*Zagrożenie cyberprzestrzeni i świata wirtualnego*" [1], którą poleca się zaangażowanemu w problematykę ochrony przed cyberprzestępczością (zob. *https://bonito.pl/produkt/zagrozenia-cyberprzestrzeni-i-swiata-wirtualnego-2?gclid=CjwKCAiAuaKfBhBtEiwAht6H76UnpO1SUfpPhmFJLaQcN19aSbvxrSdkNAW3kJ29mzfW1aW-Qc7cbRoCVckQAvD_BwE*).

Potencjalne błędy w kreowaniu oprogramowania

Zewnętrzne wnikanie w działające oprogramowanie jest konieczne, gdyż na etapach pospiesznego projektowania, programowania jak i wdrażania mogą wystąpić początkowo niedostrzeżone usterki tworzenia kodu źródłowego określonego pakietu. Skorzystajmy zatem z publikacji pod linkiem: *https://networkexpert.pl/cyberbezpieczenstwo/*, gdzie spotykamy wymienienie i zasygnalizowanie potencjalnych możliwych wystąpień błędów.

Błędy zabezpieczeń. W dobie łączności modemowej, sieci rozległych i Internetu, problemem stały się sytuacje, w których chociaż oprogramowanie działa zgodnie z oczekiwaniami projektanta, pozwala oprócz tego osobom trzecim na złośliwą interakcję z systemem. Scenariusze, które mogą prowadzić do nieautoryzowanego wykorzystania systemu, są dzielone na kilka grup, w zależności od swego pochodzenia.

Błędy projektowe. Występują wtedy, gdy założenia dla oprogramowania oparte są na błędnych przesłankach. Może to być nie w pełni poprawne rozumienie zasad funkcjonowania sieci komputerowych i budowy wykorzystywanych protokołów komunikacyjnych. Ich skutkiem może być sytuacja, w której nie można ufać wynikom pracy aplikacji i integralności przetwarzanych przez nią danych.

Błędy implementacyjne. W tej grupie błędów występują pomyłki techniczne popełniane przez programistów na skutek ich działania wywołań systemowych. Częstym efektem błędów implementacyjnych jest możliwość przejęcia pełnej kontroli nad procesem przez osoby niepowołane oraz możliwość bezpośredniej interakcji z systemem operacyjnym.

Błędy konfiguracyjne. Są to pomyłki popełniane przez administratorów, którzy przygotowują oprogramowanie do wykorzystania przez użytkowników. Przykładem może być ustawienie typowych haseł dla uprzywilejowanych kont.

Błędy operatora. Przykładem może być uruchamianie przez użytkowników załączników od niepewnych nadawców przysłanych w poczcie elektronicznej, ignorowanie komunikatów ostrzegawczych, przypadkowa zmiana opcji programu.

Monitorowanie możliwości potencjalnych zagrożeń infrastruktury krytycznej

Z punktu widzenia zagrożenia infrastruktury krytycznej w ramach organów państwa, kluczowe jest prowadzenie na bieżąco kontroli podatności systemów na ataki cyberprzestępców (zob. *https://bip.skw.gov.pl/skw/bezpieczenstwo-teleinfo/zalecenia-w-zakresie-be/5109,Zalecenia-w-zakresie-bezpieczenstwa-teleinformatycznego.html*).

W tym względzie ważna jest znajomość aspektów prawnych ochrony przede wszystkim infrastruktury krytycznej oraz faz zarządzania kryzysowego. Na uwagę zasługuje też ochrona informacji niejawnych, przy czym w szkoleniach i procedurach należy podać zasady ewakuacji obiektów lub/i obszarów należących do infrastruktury krytycznej. Zgodnie z art. 41 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa dla sektora transportu oraz sektora zaopatrzenia w wodę pitną i jej dystrybucji organem właściwym do spraw cyberbezpieczeństwa jest Minister Infrastruktury (wg: *https://www.gov.pl/web/infrastruktura/wydzial-bezpieczenstwa-teleinformatycznego*). Za realizację obowiązków organu właściwego do spraw cyberbezpieczeństwa wynikających z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa odpowiada Wydział Bezpieczeństwa Teleinformatycznego w Biurze Zarządzania Kryzysowego w Ministerstwie Infrastruktury.

Podejścia mające na celu zabezpieczenia systemów

W zabezpieczeniu systemów istotne są zbiorcze działania jakie należy podejmować, aby przeciwdziałać zagrożeniom ze strony cyberprzestępców. Skorzystajmy jeszcze z wybranych i zaimplementowanych fragmentów szerszej publikacji internetowej dotyczącej cyberbezpieczeństwa (zob. *https://networkexpert.pl/cyberbezpieczenstwo/*). Strategią zapewnienia

bezpieczeństwa systemów teleinformatycznych jest budowanie ich w sposób, który ogranicza ewentualne problemy wynikające z naruszenia zabezpieczeń lub niepożądanej aktywności uprawnionego użytkownika. Takie podejście staje się szczególnie istotne w przypadku utrzymywania dużej infrastruktury o zastosowaniu komercyjnym, a także w firmach i organizacjach rządowych. Popularnym przykładem standardu jest dwuczęściowa brytyjska norma BS 7799, *Information technology – Code of practice for information security management oraz Information Security Management Systems – Specification with guidance for use.* Norma ta została później zaadaptowana jako ISO/IEC 17799:2003 oraz ISO/IEC 27001:2005. Polskimi odpowiednikami są PN-ISO/IEC 17799:2007 oraz PN-ISO/IEC 27001:2007.

Jako przykład ograniczenia interakcji złośliwego oprogramowania, zwanego *malware* instalowany i eksploatowany jest system o nazwie *zapora sieciowa*. Oprogramowanie to stanowi narzędzie w zarządzaniu bezpieczeństwem, a jego rola ogranicza się do niezbędnego minimum zakresu możliwej interakcji między użytkownikami i systemami, oraz pomiędzy poszczególnymi komponentami określonej platformy programowej. Ponadto w analizie potencjalnych zagrożeń cyberprzestępczością istotne jest ograniczenie uprawnień nadawanych użytkownikom i systemom do najniższego, uzasadnionego realizowanymi celami poziomu, oraz taki podział kompetencji, by sfinalizowanie istotnych procesów biznesowych wymagało współpracy kilku osób.

Ważny jest też odpowiedni poziom rozliczalności i logowania działań użytkowników, a także monitorowanie tworzonych rejestrów pracy i wykrywanie innych nieprawidłowości poprzez zastosowanie programu antywirusowego. Pozwala on na reagowanie na problemy, zanim włamywacz zdecyduje się na ujawnienie swojej obecności. Trzeba jeszcze dodać, że czuwanie nad bezpieczeństwem sieci teleinformatycznych i zasobów informatycznych wzmaga okresowy *audyt wewnętrzny.*

Mimo tych przedsięwzięć wielu użytkowników obawia się o bezpieczeństwo swoich danych i prywatność podczas korzystania z Internetu. Dotychczasowe obietnice producentów sprzętu i aplikacji nie przekładają się na zauważalną redukcję liczby obserwowanych włamań, mimo tego, że około 90% użytkowników komputerów używa jakiegoś oprogramowania mającego chronić ich zasoby techniki IT przed atakami. Przed odpowiedzialnością prawną, wynikającą z zaistnienia ataku na cyberzasoby, dostawcy oprogramowania stosują niekiedy różne praktyki, a mianowicie: niezrozumiała terminologia, zrzekanie się odpowiedzialności, nie w pełni informowania o zaistniałych błędach.

Doskonalenie się specjalistów w zakresie bezpieczeństwa teleinformatycznego

Specjaliści zajmujący się bezpieczeństwem zasobów informatycznych muszą posiadać coraz szerszy zakres wiedzy, stąd też wachlarz przedmiotów wykładanych na szkoleniach w ramach Programu Akademii Bezpieczeństwa Informatycznego (EITCA/IS) obejmuje zagadnienia (wg: *https://eitca.pl/is/GISEC?gclid=CjwKCAiAuaKfBhBtEiwAht6H7-rpnAnzzJjiE55yVjnnRzx7BasqAYyAeYC-WFLFfJKe-CXcKJGNFBoCzZsQAvD_BwE)*:

- podstawy kryptografii,
- bezpieczeństwo informatyczne *e-Gospodarki*,
- administracja i zarządzanie bezpieczeństwem w systemach Microsoft,
- bezpieczeństwo systemów operacyjnych,
- bezpieczne sieci komputerowe,
- zaawansowane bezpieczeństwo sieci informatycznych,
- kryptografia kwantowa,
- formalne aspekty bezpieczeństwa informacji,
- teoria bezpieczeństwa informatycznego,
- informatyka kwantowa w kontekście bezpieczeństwa,
- złożoność obliczeniowa jako podstawa bezpieczeństwa informacji.

Główny Urząd Statystyczny w raporcie "*Społeczeństwo informacyjne w Polsce w 2021*" podał, w roku 2021 r. 95,3% przedsiębiorstw wykorzystywało przynajmniej jeden ze środków

bezpieczeństwa teleinformatycznego. W tym czasie wiele firm korzystało z usług IT świadczonych przez specjalistów z firm outsourcingowych (wg: *https://ccit.pl/bezpieczenstwo-informacji/*).

Tworząc program bezpieczeństwa oraz diagnozując potencjalne zagrożenia należy dobrać do nich odpowiednie rozwiązania zapewniające ochronę (zob. *https://twojepc.pl/news42344/Jak-zadbac-o-bezpieczenstwo-teleinformatyczne-w-firmie.html*). Jak już nadmieniono, wymienia się wśród nich różnego rodzaju programy antywirusowe, *anti-malware*, *filtry DNS*, czy nowoczesne zapory ogniowe (*firewalle*). Tego typu rozwiązania pozwalają ochronić przed atakiem nie tylko fizyczne urządzenia, ale także sieci, czy dane przechowywane w chmurze. Twórcy tych zabezpieczeń nieustannie pracują nad udoskonaleniem systemów bezpieczeństwa, których wdrożenie zapewni ochronę przed coraz nowszymi formami ataków.

Tu trzeba podkreślić, że nawet najwyższy poziom wdrożonych zabezpieczeń nie zapewni 100% ochrony, w sytuacji, gdy możliwość przeprowadzenia skutecznego cyberataku udostępni obecny lub były pracownik danego obiektu. Oczywiście często w sposób nieświadomy, ponieważ z reguły następuje to poprzez otwarcie zainfekowanego maila, czy korzystanie z sieci publicznej na służbowym sprzęcie, co może mieć miejsce podczas pracy zdalnej lub delegacji. W związku z tym należy nieustannie uświadamiać pracowników o istniejących zagrożeniach, a tego typu szkolenia powinny odbywać się regularnie. Wynika to z faktu, że najlepszą ochroną są działania prewencyjne. Podsumowując należy stwierdzić, że odpowiednia dbałość o bezpieczeństwo teleinformatyczne firmy to konieczność, która umożliwia jej bezproblemowe działania.

Środki i programy zabezpieczenia przed włamaniami cyberprzestępców

Instytucje finansowe, handlowe i nie tylko stosują różnego rodzaju rozwiązania zabezpieczające przed dostępem do kont, a przykładem są karty płatnicze z chipem (wg: *https://www.cartpoland.pl/czego-wykonany-chip-karcie-chipowej/*). Najpopularniejszą formą przechowywania informacji na karcie płatniczej są paski magnetyczne i kody kreskowe. Karty chipowe powstały przez organizację EMV zrzeszającą m.in. Europay, MasterCard i Visa. Były one odpowiedzią na niewystarczającą ochronę kart magnetycznych. Chip stał się narzędziem walki ze *skimmingiem*, czyli kopiowaniem zawartości paska magnetycznego i wykorzystywania go do zakupów na koszt ofiary, przy czym chip jest to mikroprocesor, który kontroluje dostęp do zapisanych danych. Umożliwia on ochronę procesu logowania i zapewnienie niezaprzeczalności poprzez podpis cyfrowy. Dzięki niemu przechowywane informacje są dodatkowo szyfrowane, co utrudnia ich odczytanie przez osoby niepowołane.

Przesyłanie informacji do komputera następuje wtedy, gdy odpowiednie styki w czytniku połączą się z jego powierzchnią. Mikroprocesor, kontroluje zapis i odczyt informacji wtedy, gdy w pamięci zapisywane są dane. Chip wyposażony jest też w pamięć ROM (*read-only memory*), która dzieli się na trzy obszary. Pierwszy z nich to odczyt swobodny, w którym zawarte jest imię i nazwisko posiadacza karty, jej numer oraz data ważności. Drugi to obszar poufny, który zawiera informacje o użytkowniku i dane producenta karty. Natomiast w trzecim obszarze zwanym roboczym przechowywane są informacje, które stale i dynamicznie się zmieniają. Są to saldo rachunku oraz lista operacji i transakcji.

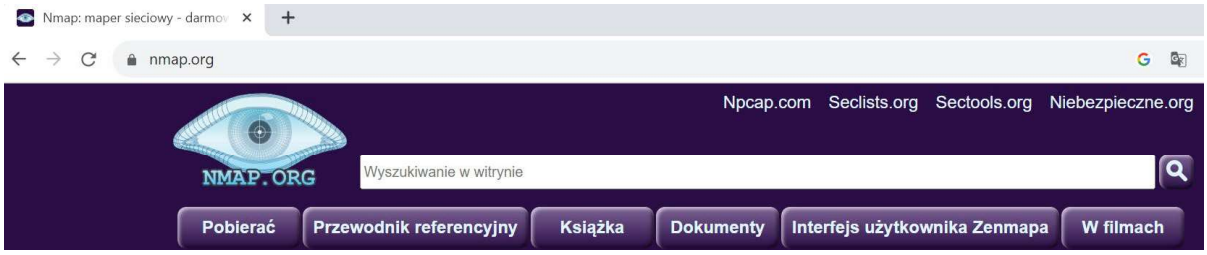
Obecnie oprócz gotówki, kart płatniczych w użyciu zaczynają być tzw. waluty cyfrowe (zob. *https://businessinsider.com.pl/technologie/waluta-przyszlosci-w-naszych-portfelach-co-to-jest-cyfrowa-waluta/g6jz7kj*). Podobnie jak Internet opanował świat, tak i nieuchronnie waluta cyfrowa, określana skrótem CBDC (*central bank digital currency*), zastąpi tradycyjne banknoty i monety, które posiadamy w portfelach. Zakłada się, że w przyszłości wirtualna waluta będzie dużym ułatwieniem dla płacących. Niektóre kraje na świecie już przeprowadzały testy w tym kierunku. W strefie euro gotowy jest projekt Europejskiego Banku Centralnego dotyczący CBDC. Szwecja, Chiny oraz Jamajka, przeprowadziły już testy obrotu CBDC. Polska też powinna podjąć się wdrażania "*e-złotówki*", bowiem CBDC to prawny środek płatniczy, tzw. programowalny pieniądz, który jest emitowany przez władzę monetarną, czyli bank centralny. W dużym uproszczeniu to banknoty i monety, którymi się teraz posługujemy, lecz w formie zdigitalizowanej.

Narzędzia przydatne w audycie bezpieczeństwa

Po tej wiadomości ze świata wirtualnego przyszłości, dotyczącej waluty cyfrowej, skupmy swoją uwagę na przykładach rozwiązań techniki IT wykrywających podatności aplikacji na zagrożenia zewnętrzne z cyberprzestrzeni. I tak *Nessus Professional* to pojedynczy skaner, który wykrywa podatności przy pomocy dwóch metod skanowania (zob. *https://www.passus.com/produkty/tenable/nessus*). Wymieniony wcześniej skaner programistyczny daje następujące możliwości:

- zapobiega atakom identyfikując podatności, które powinny zostać zlikwidowane;
- odpowiada standardom regulatorów i wymogom zgodności w najszerszym zakresie;
- umożliwia dostęp przez przeglądarkę o dowolnej porze i w dowolnym miejscu;
- posiada możliwość dostosowania raportów wg podatności lub urządzenia a także możliwość wygenerowania streszczenia dla kierownictwa lub porównania wyników różnych skanów w celu uwidocznienia zmian.

Kolejne oprogramowanie to *Nmap* (*Network Mapper*), którego ofertę pokazano na Rysunku 1. *Nmap* jest darmowym i otwartym oprogramowaniem, które stanowi narzędzie do wykrywania stanu sieci i audytu bezpieczeństwa. Wielu administratorów systemów i sieci uważa go również za przydatny do zadań takich jak inwentaryzacja sieci, zarządzanie harmonogramami aktualizacji usług i monitorowanie czasu pracy hosta lub usługi.



Rys. 1. Strona WWW programu Nmap
Źródło: http://nmap.org

Nmap wykorzystuje nieprzetworzone pakiety IP w nowatorski sposób, aby określić, jakie hosty są dostępne w sieci, jakie usługi oferują te hosty, jakie systemy operacyjne działają, jakiego typu filtry pakietów/zapory ogniowe są w użyciu i dziesiątki innych cech. Został zaprojektowany do szybkiego skanowania dużych sieci, ale działa równie dobrze dla pojedynczego hosta. Omawiany program działa na wszystkich głównych komputerowych systemach operacyjnych, a mianowicie *Linux*, *Windows* i *Mac OS X*. Oprócz klasycznego pliku wykonywalnego w postaci binarnej programu *Nmap* z wiersza poleceń możemy wywołać:

Ncat (elastyczne narzędzie do przesyłania, przekierowywania i debugowania danych),
Ndiff (narzędzie do porównywania wyników skanowania),
Nping (narzędzie do generowania pakietów i analizy odpowiedzi).

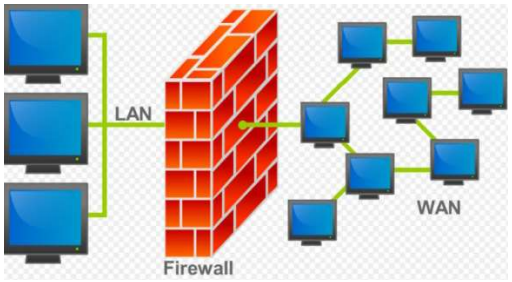
Pomocnicze środki bezpieczeństwa

Przy przesyłaniu niektórych danych stosowane są pliki w postaci zakodowanej np. w formacie ZIP jako wstępna metoda „*utajnienia*" danych [4]. ZIP jest popularnym formatem do bezstratnej kompresji i archiwizacji danych. Programy do tworzenia archiwów ZIP oferują możliwość szyfrowania danych, co jest często wykorzystywaną funkcjonalnością przy przesyłaniu plików zawierających dane osobowe pocztą e-mail.

Innym sposobem kontroli dostępu do serwera jest tzw. *Dial-up* (połączenie wdzwaniane, połączenie komutowane) – zob. *https://interneta.pl/dial-up-polaczenie-wdzwaniane/*. Jest to sposób połączenia komputera z siecią komputerową polegający na wykorzystaniu modemu telefonicznego do połączenia się z serwerem dostępowym sieci. W celu uzyskania połączenia wykorzystywana jest zwykła stacjonarna linia telefoniczna (analogowa lub cyfrowa) w postaci metalowej pętli abonenckiej lub rzadziej, jako radiowe łącze abonenckie albo bezprzewodowe łącze telefonii

komórkowej w publicznej sieci telekomunikacyjnej. Serwer dostępowy przekazuje ruch pochodzący z tak połączonego komputera do sieci komputerowej, np. sieci Internet. Tak więc połączenia wdzwaniane to usługi umożliwiające dzwonienie do innych użytkowników sieci telefonicznych z wykorzystaniem pośredniczącego numeru telefonu. Numer pośredniczący może być numerem stacjonarnym lub numerem infolinii (typu 800, 801).

Do identyfikacji elementu w sieci służy także adres IP (*IP address*). Stanowi on liczbowy identyfikator nadawany interfejsowi sieciowemu, grupie interfejsów (*broadcast*, *multicast*), bądź całej sieci komputerowej w protokole IP, służący identyfikacji elementów sieci (wg: *https://pl.wikipedia.org/wiki/Adres_IP*). Rozszerzmy jeszcze informację o zabezpieczeniu jakim jest wspomniana już zapora sieciowa (firewall) – zob. *https://pl.wikipedia.org/wiki/Adres_IP*, czyli ściana ogniowa. Jest to jeden ze sposobów zabezpieczania sieci i systemów przed atakami nieupoważnionych osób spoza sieci obiektu. Termin ten może odnosić się zarówno do sprzętu komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego niepowołany dostęp do komputera, który podlega jego ochronie. Pełni rolę połączenia ochrony sprzętowej i programowej sieci wewnętrznej LAN przed dostępem z zewnątrz, tzn. sieci publicznych, Internetu, chroni też przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz (zob. Rysunek 2). Często jest to komputer wyposażony w system operacyjny z odpowiednim oprogramowaniem. Do jego podstawowych zadań należy filtrowanie połączeń wchodzących i wychodzących oraz tym samym odmawianie żądań dostępu uznanych za niebezpieczne.



Rys. 2. Idea zapory sieciowej między LAN i WAN
Źródło: https://pl.wikipedia.org/wiki/Zapora_sieciowa#/media/Plik:Firewall.png

Zapoznajmy się jeszcze z funkcjonalnością innego typu zapory sieciowej UTM (*Unified Threat Management*) – zob. *https://www.netcomplex.pl/czym-jest-utm-zabezpiecz-siec-dzieki-zintegrowanemu-zarzadzaniu-bezpieczenstwem*. Zapora ta ma wiele funkcji ochrony brzegu sieci zgromadzonych w jednym sprzętowym urządzeniu. UTM pozwala zabezpieczyć sieć na wielu płaszczyznach. Funkcjonalność omawianej zapory nie kończy się jednak na udostępnieniu wielu narzędzi *cybersecurity* w ramach jednego rozwiązania. To także automatyzacja zarządzania wieloma procesami związanymi z utrzymaniem centrum zarządzania bezpieczeństwem danych. Z wielu powodów urządzenia UTM są podstawową składową systemu zarządzania bezpieczeństwem w średnich i mniejszych przedsiębiorstwach. Przede wszystkim mniejsze działy IT, dysponujące ograniczonym budżetem mogą dzięki wdrożeniu UTM zagwarantować ochronę najcenniejszych zasobów przedsiębiorstw, bez względu na wielkość. Zautomatyzowanie wielu czynności pozwala uniknąć zatrudnienia dodatkowych specjalistów. Tak wiec w przeciwieństwie do dużych korporacji mniejsze firmy stawiają na sprzętowy UTM z intuicyjną obsługą i szerokim wachlarzem zabezpieczeń.

Bibliografia

1. BEDNAREK J., ANDRZEJEWSKA A., *Zagrożenie cyberprzestrzeni i swiata wirtualnego*, Difin, 2014.
2. SAWICKI M., *Cyberprzestępczość*, Wydawnictwo C.H. Beck, Monografie prawnicze, 2013.
3. SHINDER D. L., Ed Tittel (Technical Editor), *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Helion, 2004.
4. SZCZEGIELNIAK-REKIEL A., KELNER J. M., *Przegląd metod szyfrowania i dekryptażu archiwum ZIP*, czasopismo: Elektronika: konstrukcje, technologie, zastosowania, Warszawa 2022, Wojskowa Akademia Techniczna, Wydział Elektroniki, CEON Biblioteka Nauki, https://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-2555200d-f18b-4187-a5c9-9f71af3b98ff.

Information about author:

Wladyslaw Wornalkiewicz – PhD, Professor ANS-WSZiA, The Academy of Applied Sciences – Academy of Management and Administration in Opole, Opole, Poland.