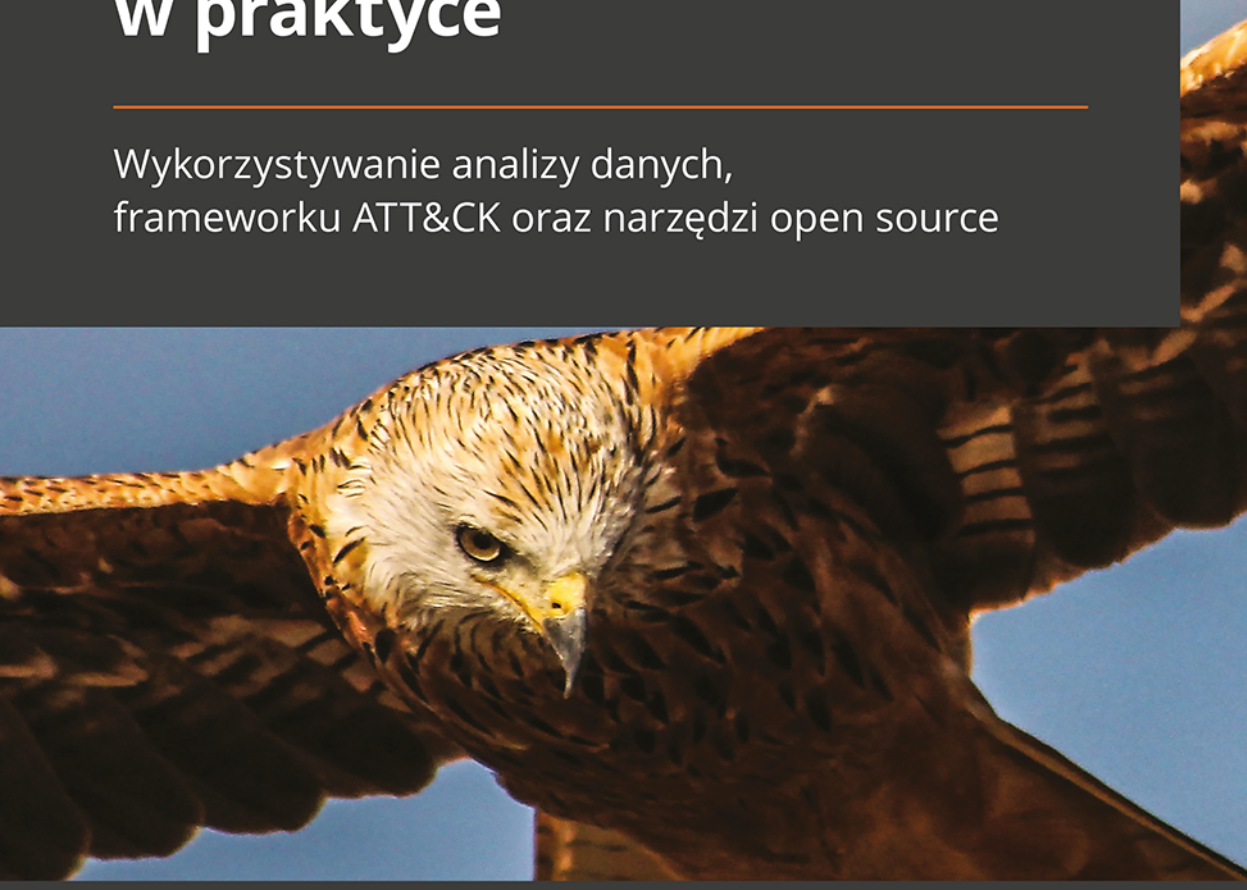
# Aktywne wykrywanie zagrożeń w systemach IT w praktyce

Wykorzystywanie analizy danych, frameworku ATT&CK oraz narzędzi open source



Valentina Costa-Gazcón

Helion

Tytuł oryginału: Practical Threat Intelligence and Data-Driven Threat Hunting
A hands-on guide to threat hunting with the ATT&CK Framework
and open source tools

Tłumaczenie: Piotr Rakowski

ISBN: 978-83-283-8885-7



Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
*https://helion.pl/user/opinie/akwyza*
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

# Spis treści

ROZDZIAŁ 3

# Z jakich źródeł pozyskujemy dane?

W celu przeprowadzenia skutecznego polowania na zagrożenia powinieneś się zapoznać z kilkoma podstawowymi pojęciami. Głównymi źródłami danych dla polowań na zagrożenia są dzienniki systemowe i sieciowe. W tym rozdziale omówimy podstawy systemu operacyjnego, podstawy sieci oraz główne źródła, z których czerpie dane platforma służąca do przeprowadzania polowań na zagrożenia.

W rozdziale tym omówimy następujące zagadnienia:

- zrozumienie zebranych danych,
- narzędzia dostępne w systemie Windows,
- źródła danych.

Zaczynajmy!

## Wymogi merytoryczne i techniczne

Do realizacji materiału z tego rozdziału potrzebny jest komputer z zainstalowanym systemem operacyjnym Windows.

## Zrozumienie zebranych danych

Polowanie na zagrożenia wymaga pracy z dziennikami zdarzeń z różnych źródeł danych. Nie ma dobrej odpowiedzi na pytanie, jaka jest właściwa ilość danych lub jakie są właściwe źródła danych, ponieważ zależy to od tego, czego szukasz i jakie są zasoby Twojej organizacji.

W każdym razie dane, które są wykorzystywane do polowania na zagrożenia, nie istnieją w próżni i są określane przez systemy operacyjne w punktach końcowych organizacji, urządzenia podłączone do sieci organizacji, a nawet poprzez wdrożone rozwiązania z zakresu bezpieczeństwa.

W poprzednich rozdziałach stwierdziliśmy, że częścią zestawu umiejętności łowcy zagrożeń jest zdolność do zrozumienia architektury sieci i rozpoznania nietypowych wzorców zarówno w aktywności sieciowej, jak i w danych zbieranych z punktów końcowych i aplikacji. Zanim więc przyjrzymy się samym źródłom danych, krótko omówmy kilka podstaw dotyczących systemów operacyjnych i sieci.

## Podstawy systemów operacyjnych

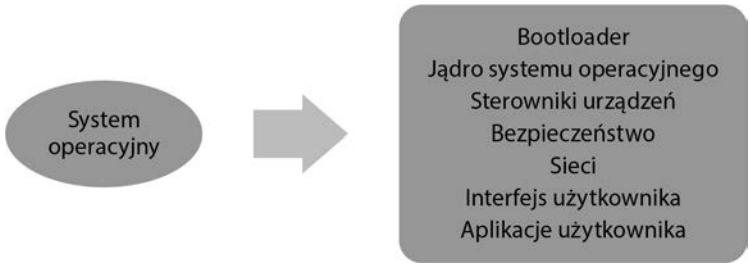
**System operacyjny** jest częścią oprogramowania, która jest warstwą pośrednią pomiędzy człowiekiem a sprzętem komputerowym. Oprócz zarządzania oprogramowaniem i sprzętem system operacyjny jest również odpowiedzialny za określanie zasobów, które są przydzielane każdemu procesowi. Koordynuje on różne programy, które próbują uzyskać dostęp do tych samych zasobów w tym samym czasie.

Istnieją różne rodzaje systemów operacyjnych w zależności od ich funkcjonalności: **systemy operacyjne czasu rzeczywistego** (tzw. RTOS); **jednozadaniowe — przeznaczone dla jednego użytkownika**; **wielozadaniowe — przeznaczone dla jednego użytkownika**; a także **wielozadaniowe — przeznaczone dla wielu użytkowników**. Obecnie najczęściej używane są wielozadaniowe systemy operacyjne.

Trzy najczęściej spotykane wielozadaniowe systemy operacyjne dla komputerów to Windows, macOS i Linux, przy czym Windows ma największy udział w rynku (80%), za nim plasuje się macOS (10%), a następnie Linux (2%). Pomimo wielu różnic wszystkie one wykonują pewien wspólny zakres zadań, które można podsumować w sposób pokazany na rysunku 3.1.


**Rysunek 3.1.** Podstawowa architektura systemu operacyjnego

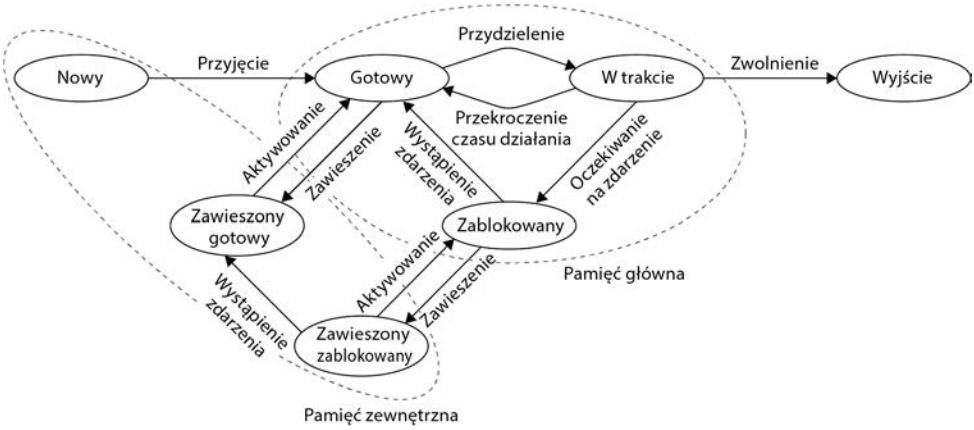
Zaraz po włączeniu komputera pamięć **ROM** (ang. *Read-Only Memory*) sprawdza, czy wszystkie komponenty sprzętowe działają prawidłowo, wykonując tzw. test **POST** (ang. *Power-On Self-Test*). Następnie oprogramowanie w pamięci ROM, zwane **podstawowym systemem zarządzania urządzeniami wejścia-wyjścia** (ang. *Basic Input-Output System*, BIOS), aktywuje dyski, zanim **bootloader** załaduje system operacyjny do pamięci (rysunek 3.2).




**Rysunek 3.2.** Podstawowe komponenty systemu operacyjnego

Zadania wykonywane przez system operacyjny można podzielić na sześć kategorii:

1. **Zarządzanie mikroprocesorem.** System operacyjny musi zapewnić, aby każdy proces otrzymał wystarczająco dużo czasu (cykli mikroprocesora), aby móc prawidłowo funkcjonować. **Proces** można zdefiniować jako część oprogramowania wykonującą działanie, które można kontrolować. System operacyjny *planuje* procesy do wykonania przez mikroprocesor, który może obsłużyć tylko jeden proces w tym samym czasie (rysunek 3.3).




**Rysunek 3.3.** Stany procesów w systemach operacyjnych

System operacyjny przełącza się pomiędzy procesami z niewiarygodną prędkością, co powoduje zachowanie wrażenia ciągłości działania.

2. **Zarządzanie pamięcią.** System operacyjny musi zapewnić, aby każdy uruchomiony proces otrzymał wystarczającą ilość pamięci, ale zarządzanie pamięcią odnosi się również do odpowiedniego wykorzystania różnych typów pamięci.

Zazwyczaj, gdy mówimy o zarządzaniu pamięcią, odnosimy się do trzech różnych typów pamięci:

a) **Bardzo szybka pamięć cache**, znana również jako pamięć procesora. Jest to bardzo szybka pamięć **SRAM** (ang. *Static Random Access Memory*), do której dostęp można uzyskać za pomocą naprawdę szybkich interfejsów. Są to niewielkie ilości zasobów pamięci wykorzystywane do przechowywania danych, które najprawdopodobniej będą potrzebne procesorowi w celu zwiększenia wydajności działania procesora.

b) **Pamięć główna**, znana również jako **RAM** (ang. *Random Access Memory*). Jest to miejsce, w którym informacje są przechowywane, gdy procesor z nich korzysta. System operacyjny pobiera informacje z pamięci zewnętrznej do pamięci RAM, gdy program jest uruchamiany.

c) **Pamięć zewnętrzna.** Jest to pamięć masowa, w której wszystkie aplikacje i dostępne informacje pozostają, gdy nie są używane.

3. **Zarządzanie urządzeniem.** Menedżer urządzeń jest odpowiedzialny za zarządzanie urządzeniami wejścia-wyjścia (I/O). Zwykle wiąże się to z wykorzystaniem **sterowników**. Sterownik to element oprogramowania, który umożliwia komunikację z urządzeniem wejścia-wyjścia, takim jak klawiatura, mysz, drukarka, mikrofon itd., bez konieczności znajomości wszystkich specyfikacji sprzętu komputerowego. Można powiedzieć, że sterownik działa jako tłumacz między warstwą sprzętową urządzenia działającą na poziomie niskim a systemem operacyjnym komputera działającym na poziomie wysokim. System operacyjny śledzi podłączone urządzenia i jego sterowniki, monitoruje statusy urządzeń i zarządza ich dostępem do zasobów komputera.
4. **Zarządzanie pamięcią masową.** Jak sama nazwa wskazuje, jest to miejsce, gdzie zarządza się sprzętem, który jest używany do przechowywania danych generowanych przez użytkownika/system. Proces ten stara się zoptymalizować wykorzystanie pamięci masowej i chronić integralność danych. Mechanizm, który jest używany do dostępu do tych danych, jest nazywany **systemem plików**.
5. **Interfejs aplikacji. Interfejs programistyczny aplikacji** (API) to zestaw procedur i protokołów, które pomagają programistom korzystać z usług systemu operacyjnego bez konieczności znajomości wszystkich specyfikacji komputera. API są implementowane przez wywołania funkcji o określonej składni. Więcej o Windows API można przeczytać na stronie Microsoftu: *https://docs.microsoft.com/en-us/windows/win32/apiindex/api-index-portal/*.
6. **Interfejs użytkownika.** Jak sama nazwa wskazuje, interfejs *użytkownika* zapewnia strukturę, dzięki której może zachodzić interakcja między użytkownikiem a komputerem. Istnieją interfejsy oparte na tekście, takie jak powłoki systemowe, oraz **graficzne interfejsy użytkownika** (GUI). Celem **interfejsów użytkownika** jest pomoc użytkownikowi w obsłudze komputera. Różnice w *wyglądzie i działaniu* różnych systemów operacyjnych są najbardziej oczywistym elementem rozróżniającym te systemy z punktu widzenia przeciętnego użytkownika.

Ważne jest, aby pamiętać, że funkcjonalność systemu operacyjnego i jego zadania to złożony i fascynujący temat, który jednak wykracza poza zakres tej książki. Gorąco polecamy kontynuowanie nauki na ten temat poprzez zapoznanie się z doskonałymi lekturami, takimi jak *Podstawy systemów operacyjnych* Abrahama Silberschatza oraz *Operating Systems Design and Implementation* Andrew S. Tanenbauma i Alberta S. Woodhulla. Dostępne są również interesujące książki dla konkretnych systemów operacyjnych, takie jak *Windows od środka* Marka Russinovicha, Alexa Ionescu, Davida A. Solomona i Pavla Yosifovicha czy *Understanding the Linux Kernel* Daniela Boveta.

Niezależnie od tego, jaki system operacyjny jest uruchomiony, czy będzie to system działający na komputerze, czy na urządzeniu mobilnym, atakujący zawsze będzie ograniczony właśnie przez system operacyjny, który jest uruchomiony na danym urządzeniu. Złośliwe oprogramowanie może uruchomić jakiś proces lub zamaskować to, co robi, kryjąc się pod innymi uruchomionymi procesami, ale nie może zmienić sposobu działania systemu operacyjnego ani zadań, które powinien on wykonywać, aby funkcjonować poprawnie. W tej książce skupimy się głównie na systemie operacyjnym Windows i jego źródłach danych.

## Podstawy działania sieci komputerowych

Ta książka nie jest poświęcona sieciom. Nie jest też moim zamiarem przedstawienie rozprawy na ten temat, ale ponieważ część pracy łowcy zagrożeń polega na interpretowaniu dzienników sieciowych, przyjrzyjmy się kilku podstawowym pojęciom dotyczącym sieci.

### Czym jest sieć?

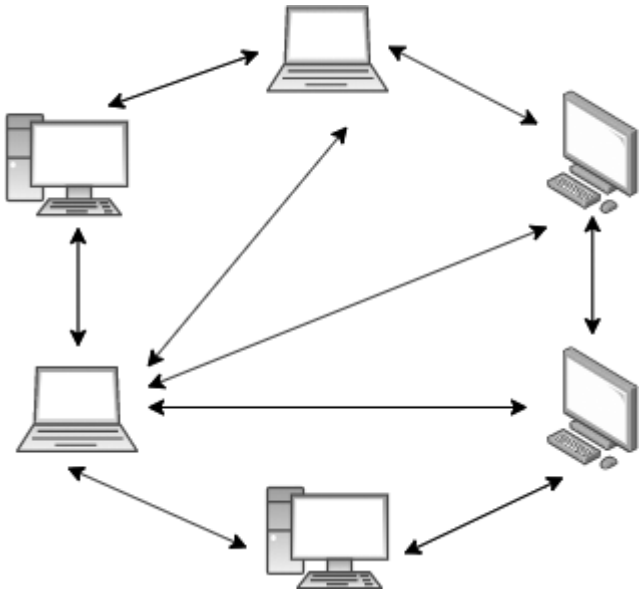
W dzisiejszych czasach mówimy o *internecie* i używamy słowa *sieć*, tak jakby były to pojęcia zamienne, ale to nie jest poprawne. W pewnym sensie internet jest siecią sieci. Inaczej mówiąc, **sieć** jest zbiorem dwóch lub większej liczby urządzeń komputerowych połączonych ze sobą w celu wymiany danych. Każde urządzenie w sieci nazywane jest **węzłem**, a połączenie między nimi może być bezprzewodowe lub wykonane za pomocą fizycznego kabla. Aby komunikacja była skuteczna, muszą być spełnione pewne warunki. Po pierwsze, wszystkie urządzenia muszą być identyfikowane w sposób jednoznaczny (unikalny). Po drugie, wszystkie urządzenia powinny mieć zaimplementowane wspólne standardowe sposoby „rozumienia" siebie nawzajem (protokoły).

Sieci można podzielić ze względu na ich **topologię** (**magistrala**, **gwiazda**, **pierścień**, przy czym obecnie najbardziej popularną topologią jest gwiazda) lub ze względu na ich **architekturę** (***peer-to-peer*** i **klient-serwer**). Sieci mogą być również **publiczne** (dostępne dla każdego, kto korzysta z internetu) lub **prywatne**.

### Peer-to-peer (P2P)

Sieć ***peer-to-peer*** (P2P) składa się z systemów komputerowych (peerów) połączonych ze sobą za pośrednictwem internetu bez potrzeby korzystania z centralnego serwera. Każdy komputer równorzędny jest zarówno serwerem plików, jak i klientem. Część zasobów

każdego komputera (moc obliczeniowa, pamięć dyskowa, przepustowość sieci) jest dzielona pomiędzy sieci. Wszystkie węzły mają te same prawa i obowiązki, ale żaden z nich nie ma władzy nad pozostałymi. Rysunek 3.4 ilustruje przykład tego typu sieci.



**Rysunek 3.4.** Sieć P2P

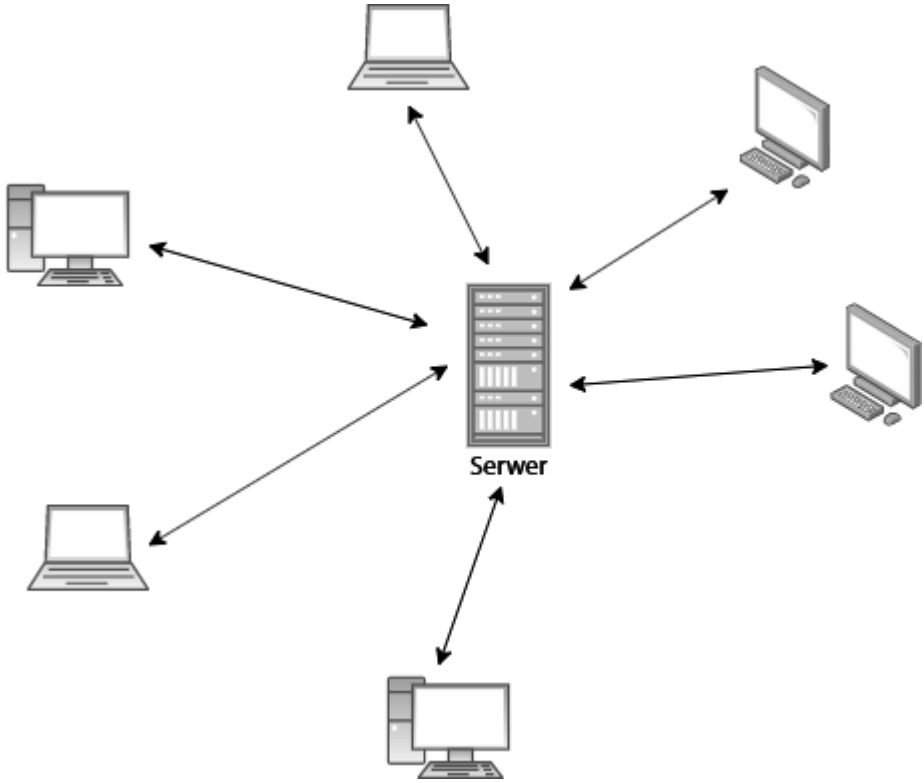
Ten rodzaj sieci jest idealny do wymiany plików między użytkownikami. Po zainstalowaniu oprogramowania P2P użytkownik może wyszukiwać pliki na komputerach innych osób, zazwyczaj w określonym katalogu wybranym przez peera. W ten sposób działały takie programy do wymiany plików jak Napster czy Kazaa. Platformy torrentowe korzystają z podobnego mechanizmu, choć w tym przypadku plik jest pobierany na komputer w odcinkach, które pochodzą z tylu komputerów, ile jest w posiadaniu tego samego pliku.

Odłączenie węzła od sieci nie spowoduje jej zniszczenia, a dodawanie nowych peerów jest proste. Dodatkowo każdy nowy peer zwiększa prędkość sieci. Tak więc gdy mówimy o sieci P2P, więcej oznacza naprawdę lepiej! Z drugiej strony sieci P2P mogą być wykorzystywane do rozpowszechniania złośliwego oprogramowania, poufnych lub prywatnych informacji i są szczególnie podatne na ataki typu odmowa usługi (*Denial of Service*).

## Klient-serwer

Jak wiemy, w przypadku **sieci typu klient-serwer** mamy do czynienia z siecią komputerową, w której jeden scentralizowany komputer (serwer) jest rdzeniem, do niego zaś podłącza się wiele innych komputerów (klientów). Klienty te wysyłają żądania w celu uzyskania dostępu do programów lub informacji przechowywanych na serwerze. W tego typu sieci klienty nie współdzielą swoich zasobów ani z serwerem, ani z innymi węzłami sieci.

Ten typ sieci pozwala na lepszą dystrybucję informacji lub aplikacji, które muszą być utrzymywane przez administratora ze scentralizowanego punktu widzenia (organizacja lub firma). Jeśli chodzi o bezpieczeństwo, ponieważ wszystkie informacje są zgromadzone w jednym miejscu, poziom kontroli nad tym, co się z nimi robi, jest znacznie wyższy, podobnie jak mechanizm implementacji ich zabezpieczenia. Z drugiej strony, jeśli serwer otrzyma zbyt wiele żądań w tym samym czasie, może dojść do przeciążenia systemu, co oznacza, że informacje pozostaną niedostępne. Ten rodzaj sieci wymaga również wyższych kosztów utrzymania i zasobów niż sieci P2P (rysunek 3.5).



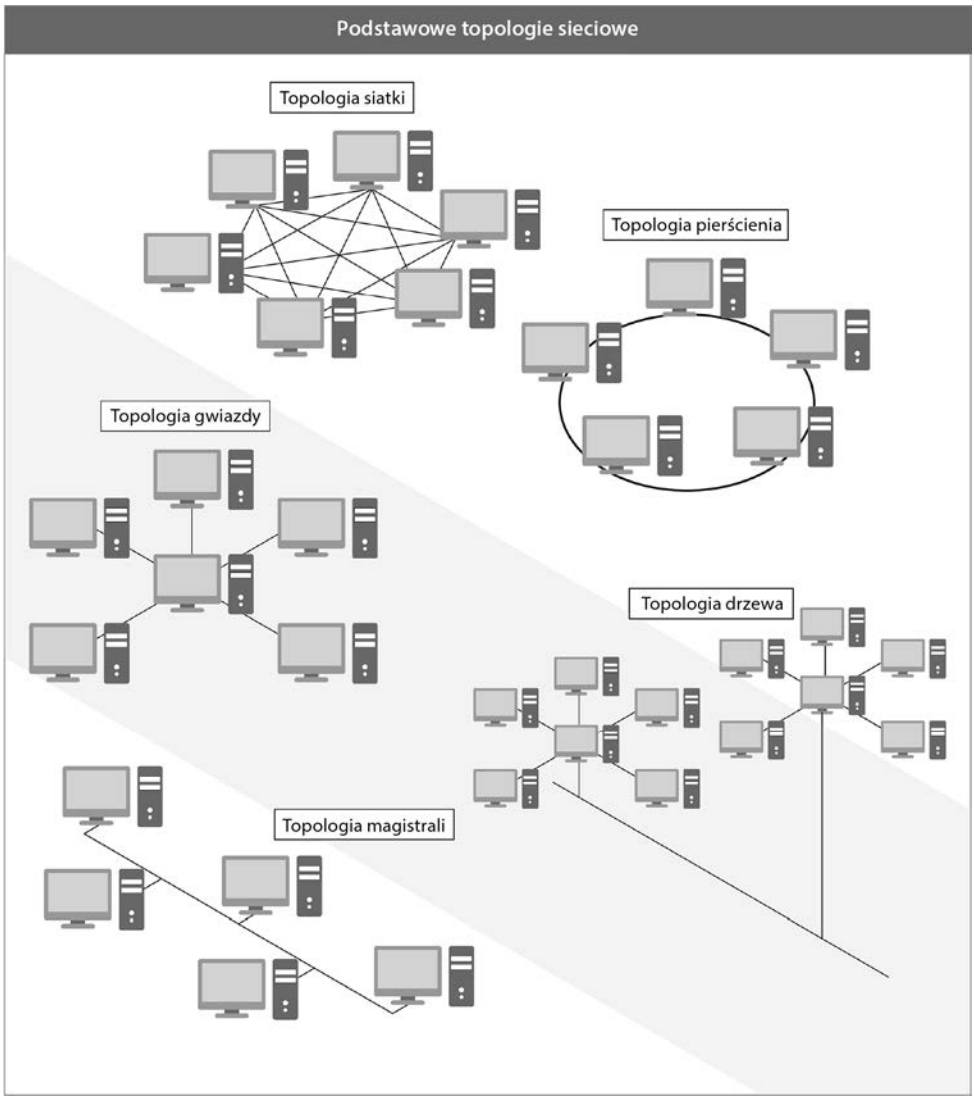

**Rysunek 3.5.** Sieć typu klient-serwer

Rysunek 3.6 pokazuje przykłady różnych topologii sieci, z którymi możesz się spotkać.

Należy pamiętać, że mogą być one również łączone w tzw. **topologię hybrydową**.

## Rodzaje sieci komputerowych

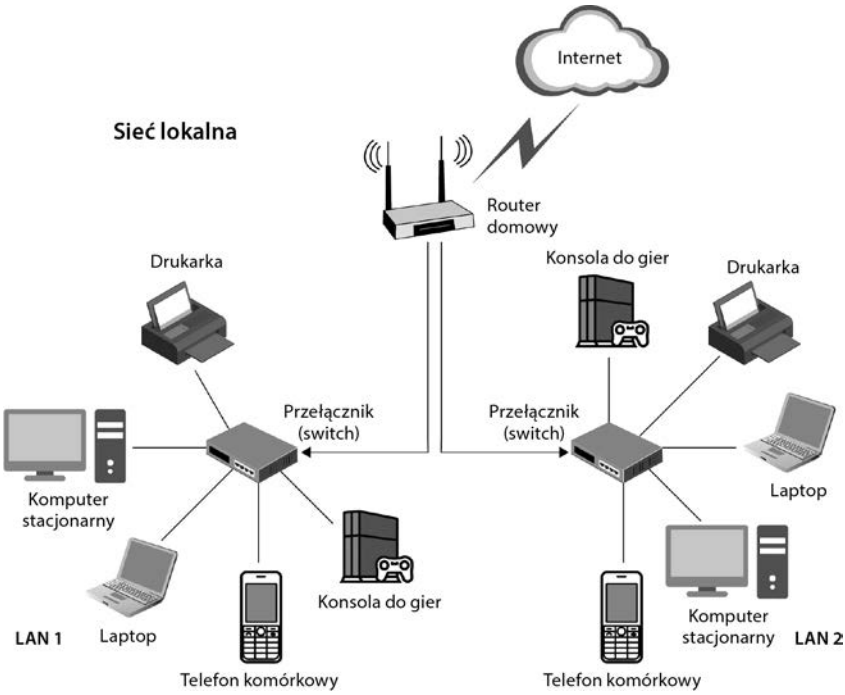
W tej części omówimy różne rodzaje sieci: **wirtualne sieci lokalne** (VLAN), **sieci osobiste** (PAN), **sieci metropolitalne** (MAN), **sieci rozległe** (WAN) oraz **sieci lokalne** (LAN).




**Rysunek 3.6.** Topologie sieciowe

## Sieci LAN

Termin **LAN** (ang. *Local Area Network*) jest używany w odniesieniu do sieci, która łączy niewielką liczbę urządzeń komputerowych znajdujących się w niewielkiej odległości od siebie. Z tego typu sieci korzysta większość domów i firm. Termin **WLAN** jest używany w odniesieniu do *bezprzewodowej sieci LAN*. Ogólnie rzecz biorąc, połączenia przewodowe (poprzez kable Ethernet) znacznie szybciej transmitują dane niż połączenia bezprzewodowe (rysunek 3.7).




**Rysunek 3.7.** Przykład sieci LAN

Przyjrzyjmy się teraz **sieciom rozległym** (WAN).

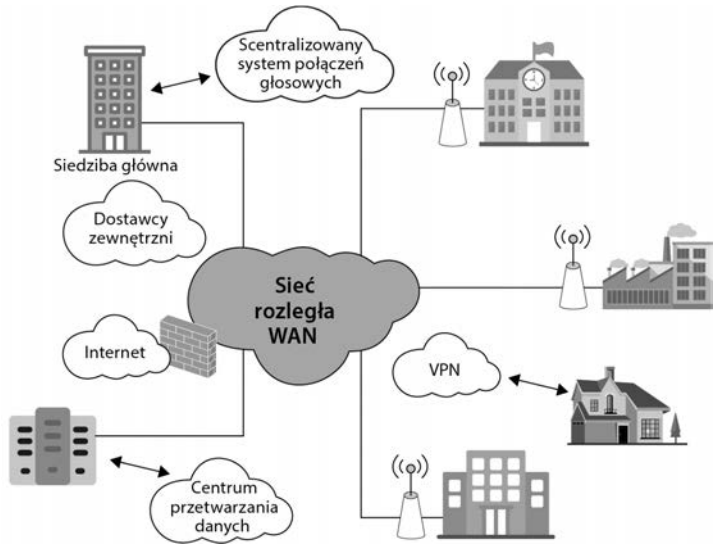
## Sieci WAN

Sieci **WAN** (ang. *Wide Area Network*) to sieci, które łączą dwie lub więcej sieci LAN na większym obszarze, umożliwiając współdzielenie danych między odległymi lokalizacjami. Zazwyczaj termin *WAN* jest używany w odniesieniu do sieci na poziomie państwa, województwa lub powiatu — na przykład **dostawca usług internetowych** (ang. *Internet Service Provider*, ISP) działa w sieci WAN. Sieci WAN mogą być również budowane do użytku prywatnego przez firmy i organizacje (rysunek 3.8).

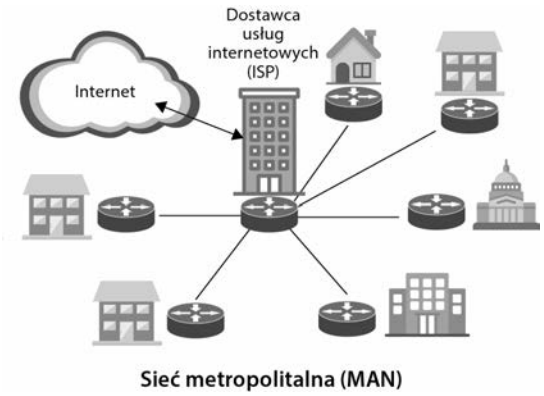
Następnie zajmiemy się **sieciami metropolitalnymi** (MAN).

## Sieci MAN

Termin **MAN** (ang. *Metropolitan Area Network*) jest używany w odniesieniu do infrastruktury sieciowej, która została opracowana dla dużych miast. Działanie tych sieci polega na połączeniu ze sobą wielu sieci LAN. Sieci MAN są punktem pośrednim pomiędzy sieciami LAN a WAN. Sieci MAN są zazwyczaj ograniczone do miast lub miasteczek (rysunek 3.9), podczas gdy WAN obejmują znacznie większy obszar.




**Rysunek 3.8.** Przykład sieci WAN

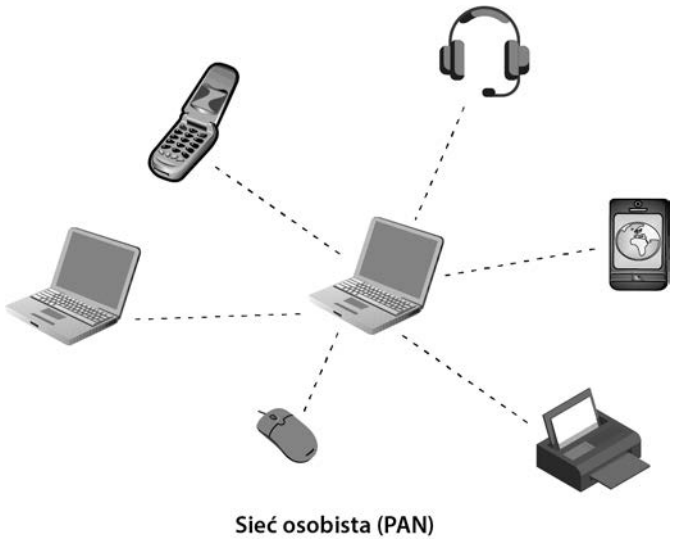



**Rysunek 3.9.** Przykład sieci MAN

Kolejnym typem sieci są **sieci osobiste** (PAN).

## Sieci PAN

Termin **PAN** (ang. *Personal Area Network*) jest używany w odniesieniu do sieci komputerów osobistych, które są tworzone poprzez podłączenie urządzeń osobistych, takich jak smartfony, klawiatura, mysz, tablety, drukarki, słuchawki, urządzenia noszone na ciele (ang. *wearables*) i inne, do komputera osobistego. Ten typ sieci ma zazwyczaj bardzo ograniczony zasięg (rysunek 3.10). Jeśli połączenie jest realizowane bezprzewodowo, mówimy o **bezprzewodowej sieci osobistej** (ang. *Wireless Personal Network*, WPAN), która czasami wymaga użycia technologii Bluetooth (fale radiowe krótkiego zasięgu) lub połączeń w podczerwieni (światło podczerwone).




**Rysunek 3.10.** Przykład sieci PAN

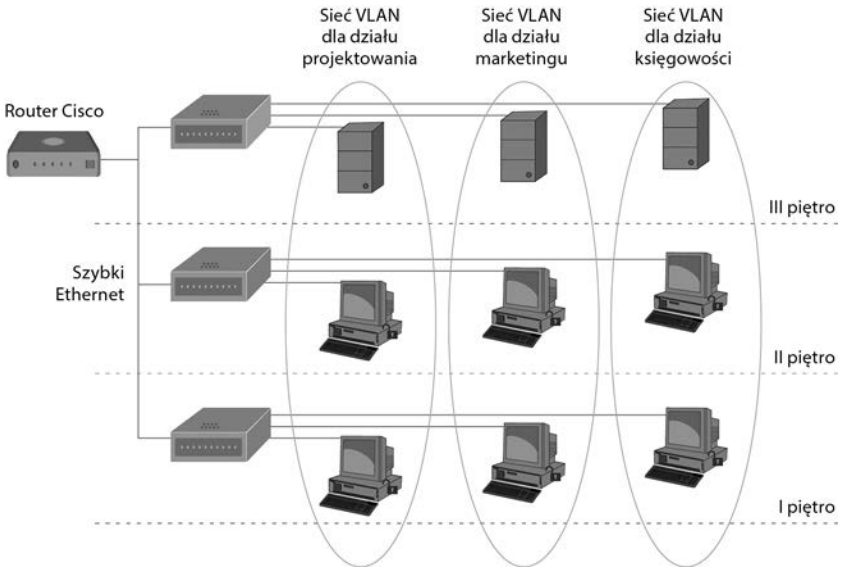
Ostatnim typem sieci są **wirtualne sieci lokalne** (VLAN).

## Sieci VLAN

Termin **VLAN** (ang. *Virtual Local Area Network*) odnosi się do konfiguracji urządzeń podłączonych do jednej lub większej liczby sieci LAN, która sprawia, że komunikują się one tak, jakby były podłączone do tego samego kabla. Sieci VLAN są zwykle obsługiwane przez przełączniki sieciowe. Służą one do segregacji ruchu w odizolowanych wirtualnych sieciach LAN, które nie mogą się ze sobą komunikować. Mogą być również używane do ograniczania lokalnego dostępu do urządzeń.

W statycznych sieciach VLAN każdy port przełącznika jest przypisany do sieci wirtualnej. Podłączone urządzenia automatycznie stają się częścią powiązanej sieci VLAN. W dynamicznych sieciach VLAN urządzenia są powiązane z siecią VLAN na podstawie swoich właściwości. Aby dwie sieci VLAN mogły się ze sobą komunikować, stosuje się routery lub przełączniki warstwy trzeciej, które „wiedzą", że działają w sieci VLAN (rysunek 3.11).

Każdy komputer będący członkiem sieci LAN może zobaczyć informacje, które są transmitowane w sieci. W przypadku przesyłania poufnych informacji umieszczanie w jej obrębie tylko użytkowników o odpowiednim poziomie uprawnień może być sposobem na zmniejszenie ryzyka naruszenia bezpieczeństwa. Sieci VLAN oferują dodatkową warstwę zabezpieczeń, która jest korzystna dla firm i organizacji, gdyż pozwala im na bardziej efektywne skalowanie i segmentowanie sieci. Ponadto segmentacja pomaga zapobiegać kolizjom pakietów i zatorom w sieci.




**Rysunek 3.11.** Przykład sieci VLAN

## Bramy sieciowe

**Brama sieciowa** (ang. *network gateway*) to nazwa nadana mechanizmom, które działają jako łączniki pomiędzy różnymi sieciami. Brama sieciowa może być formą oprogramowania, elementem sprzętu lub jednym i drugim. Komponent sprzętowy, który umożliwia komputerowi podłączenie się do sieci, jest znany jako **karta interfejsu**. Przyjrzyjmy się kilku bramom sieciowym:

- **Hub.** Hub to sprzętowe urządzenie **sieciowe**, które zawiera wiele urządzeń Ethernet, stąd też posiada wiele portów. Huby działają jako pojedynczy segment sieci. Technologia ta została zastąpiona przez przełączniki sieciowe.
- **Przełącznik** (ang. *switch*)**.** Przełącznik jest sieciowym urządzeniem sprzętowym, które używa techniki *przełączania pakietów* podczas odbierania i przekazywania danych, zapewniając, że tylko urządzenie, które potrzebuje danych, otrzyma te dane. Przełączniki sieciowe wykorzystują adresy MAC w pakietach do przekazywania danych w warstwie łącza lub w warstwie sieci.
- **Most.** Most jest urządzeniem sieciowym, które łączy dwie oddzielne sieci tak, jakby były tą samą siecią. Mosty mogą być również *mostami bezprzewodowymi*.
- **Router.** Router to urządzenie sprzętowe, które umożliwia komunikację z internetem. Służy on jako pośrednik między dostawcą usług internetowych a internetem, ale jest używany również do konfigurowania sieci LAN. Routery mogą łączyć dwie lub więcej sieci w tym samym czasie, ale obsługiwać je jako oddzielne jednostki.

W ten sposób poznaliśmy bramy sieciowe. Teraz przyjrzyjmy się zagadnieniu **translacji adresów sieciowych** (NAT).

## NAT

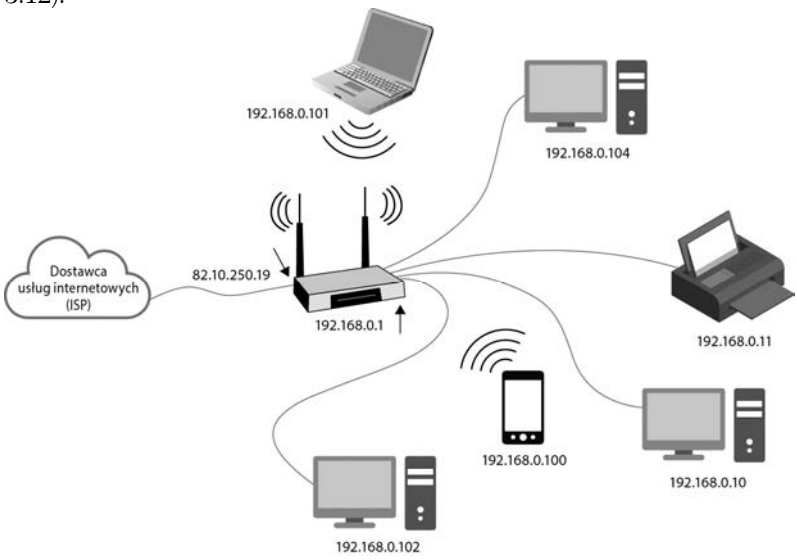
**NAT** (ang. *Network Address Translation*) to nazwa procesu, w którym router lub inne urządzenie sieciowe przypisuje adres IP do urządzeń sieciowych wewnątrz sieci.

**Adres IP** to szereg liczb oddzielonych kropkami, które służą jako identyfikator węzła sieci. Istnieją dwa rodzaje adresów IP: **IPv4** i **IPv6**. W protokole IPv4 dostępnych jest $2^{32}$ różnych kombinacji 32-bitowych adresów. Protokół IPv6 jest rozwijany od 1994 r. w celu zaspokojenia zapotrzebowania na większą liczbę adresów IP. IPv6 udostępnia $2^{128}$ kombinacji adresów 128-bitowych. Oprócz rodzaju adresu IP możemy również rozróżnić **prywatne adresy IP** i **publiczne adresy IP**. Oba są potrzebne, jeśli chcesz się połączyć z internetem.

Traktuj router jak drzwi wejściowe do budynku. Główne drzwi mają publiczny numer, który mogą zobaczyć wszyscy ludzie na ulicy (na przykład *123*), a wewnątrz budynku może się znajdować grupa mieszkań oznaczonych jako A, B i C. Następny budynek na ulicy będzie miał również numer przypisany do jego drzwi wejściowych, ale nie będzie to taki sam numer jak numer pierwszego budynku. Jednak druga grupa mieszkań w budynku może być również oznaczona literami A, B i C. Coś podobnego dzieje się z routerami w odniesieniu do publicznych i prywatnych adresów IP.

Publiczny adres IP jest zawsze unikalny dla każdego węzła w internecie. Od strony publicznej wszystkie urządzenia w sieci mają ten sam adres IP, ale za każdym razem gdy urządzenie dostaje odpowiedź z internetu, router jest odpowiedzialny za kierowanie odpowiedzi do urządzenia, które wysłało żądanie. Aby to zrobić, router musi pamiętać *stan* połączenia (porty, kolejność pakietów i adresy IP).

Prywatne adresy IP są definiowane wcześniej i powinny się zawierać w przedziale od 10.0.0.0 do 10.255.255.255, od 172.16.0.0 do 172.31.255.255 lub od 192.168.0.0 do 192.168.255.255 (rysunek 3.12).




**Rysunek 3.12.** Adres publiczny oraz prywatne adresy IP w sieci domowej

Następnie przyjrzymy się protokołom sieciowym.

## Protokoły

**Protokół sieciowy** to zestaw reguł i sygnałów, których komputery używają do komunikacji w sieci. Model OSI, który określa i standaryzuje komunikację pomiędzy różnymi systemami komputerowymi, wyróżnia siedem abstrakcyjnych warstw (rysunek 3.13). Protokoły mogą być klasyfikowane według warstwy, do której należą.

| | | |
|---|---|---|
| 7 | Warstwa aplikacji | Warstwa interakcji człowiek – komputer, w której aplikacje mają dostęp do usług sieciowych |
| 6 | Warstwa prezentacji | Zapewnia, że dane są w użytecznym formacie, i to w tej warstwie następuje szyfrowanie danych |
| 5 | Warstwa sesji | Utrzymuje połączenia i jest odpowiedzialna za kontrolę portów i sesji |
| 4 | Warstwa transportu | Przesyła dane za pomocą protokołów transmisyjnych, w tym TCP i UDP |
| 3 | Warstwa sieci | Decyduje o tym, jaką fizyczną ścieżką będą przesyłane dane |
| 2 | Warstwa łącza danych | Określa format danych w sieci |
| 1 | Warstwa fizyczna | Przesyła nieprzetworzony strumień bitów przez nośnik fizyczny |

**Rysunek 3.13.** Model OSI

Poniżej znajduje się krótka, niewyczerpująca lista kilku podstawowych protokołów, z którymi należy się zapoznać:

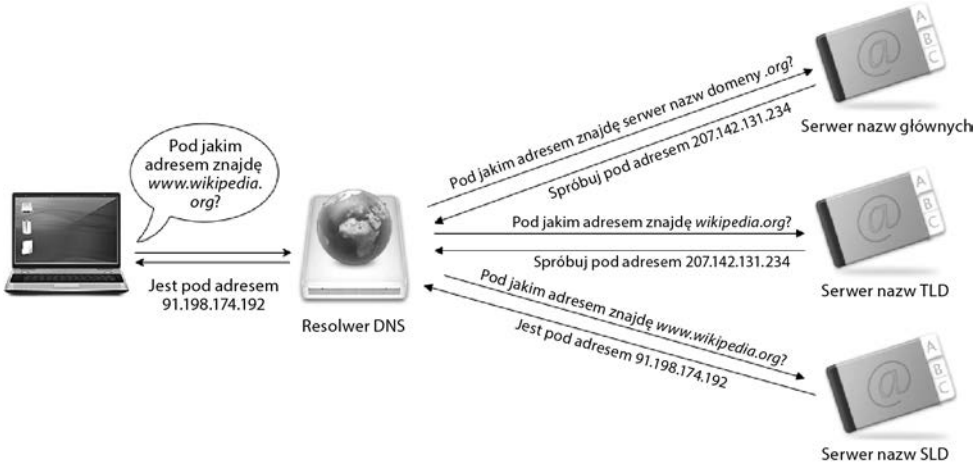
- **Protokół DHCP** (ang. *Dynamic Host Configuration Protocol*)**.** DHCP jest protokołem odpowiedzialnym za przydzielanie urządzeniom adresów IP. DHCP jest częścią warstwy aplikacji. Serwerem DHCP jest każdy komputer w sieci śledzący adresy IP, które mogą zostać przydzielone. Za każdym razem, gdy urządzenie łączy się z siecią, automatycznie żąda adresu IP. Ten adres IP będzie związany z urządzeniem przez określony czas, a kiedy jego czas się skończy, zostanie mu przydzielony nowy adres. Wszystko to dzieje się bez ingerencji użytkownika.
- **Protokół internetowy IP** (ang. *Internet Protocol*)**.** IP jest głównym protokołem komunikacyjnym w internecie. Protokół ten pomaga w trasowaniu i adresowaniu **pakietów** danych tak, aby były one dostarczane do właściwego miejsca przeznaczenia. Ogólnie rzecz biorąc, protokół ten jest używany w połączeniu z innymi protokołami transportowymi, które określają ilość danych zawartych

w pakiecie w celu zapewnienia ich prawidłowego dostarczenia. Dowiedzmy się trochę więcej o tych pakietach:

- Każdy pakiet IP jest tworzony przez nagłówek, w którym podane są różne adresy źródłowe i docelowe oraz całkowita długość pakietu w bajtach, **czas życia pakietu** (ang. *Time-to-Live*, TTL) lub liczba węzłów sieciowych, przez które wolno przejść pakietowi, zanim zostanie odrzucony, a także informacja o protokole transportowym, który ma być używany. Jego maksymalny rozmiar to 64 kB.
- Kilka protokołów pomaga kierować pakiety danych przez internet w oparciu o docelowy adres IP. Routery posiadają w swojej konfiguracji **tablice routingu**, mówiące im, w którą stronę powinny wysyłać pakiety. Pakiety będą przechodziły przez różne węzły (**systemy autonomiczne**) w sieci, aż dotrą do węzła odpowiedzialnego za docelowy adres IP, który będzie kierował pakiety wewnętrznie, aż dotrą do ostatecznego celu.

- **Protokół sterowania transmisją TCP/IP** (ang. *Transmission Control Protocol*)**.** TCP jest protokołem transportowym. Określa on sposób, w jaki dane są wysyłane i odbierane. Kiedy używany jest TCP, nagłówek pakietu zawiera sumę kontrolną, aby wskazać kolejność, w jakiej pakiety mogą być ułożone po ich otrzymaniu. TCP otwiera połączenie z odbiorcą pakietów przed rozpoczęciem transmisji. Odbiorca potwierdza nadejście każdego z tych pakietów. Jeśli potwierdzenie nie zostanie odebrane, TCP wysyła pakiet ponownie, aż do momentu, gdy jego odbiór się powiedzie. Protokół TCP został zaprojektowany w celu zapewnienia niezawodności.
- **Protokół datagramów użytkownika UDP/IP** (ang. *User Datagram Protocol*)**.** UDP jest również protokołem transportowym, który został zaprojektowany tak, aby był szybszy niż TCP, ale mniej niezawodny. W porównaniu do TCP, UDP nie sprawdza, czy pakiety dotarły do miejsca przeznaczenia lub czy zostały dostarczone w odpowiedniej kolejności. Ponadto nie nawiązuje połączenia z miejscem przeznaczenia przed wysłaniem pakietów. Ten protokół transportowy został szeroko zaadaptowany do przesyłania strumieniowego audio i wideo.
- **Hypertext Transfer Protocol (HTTP)** i **Hypertext Transfer Protocol Secure (HTTPS).** HTTP i HTTPS są prawdopodobnie najbardziej znanymi protokołami warstwy aplikacji, które są kojarzone przez przeciętnego użytkownika, ponieważ są one wykorzystywane do przeglądania stron internetowych. Te dwa protokoły umożliwiają przesyłanie danych przez internet. HTTP pozwala językowi HTML i innym językom skryptów internetowych, takim jak JavaScript i CSS, na poruszanie się między przeglądarkami. HTTPS jest bezpieczną wersją protokołu HTTP, która umożliwia szyfrowanie komunikacji między klientem a serwerem za pomocą protokołu **TLS** (ang. *Transport Layer Security*) lub **SSL** (ang. *Secure Sockets Layer*).
- **System nazw domen DNS** (ang. *Domain Name System*)**.** System DNS jest często określany mianem *internetowej książki telefonicznej*. Ludziom trudno jest zapamiętać adresy IP. Dlatego też, wchodząc na strony internetowe, zamiast wpisywać adres IP, wpisujemy *nazwę domeny*, która zostanie przetłumaczona przez protokół DNS na adres IP strony. Internet, jaki znamy, nie istniałby bez protokołu DNS.

Gdy użytkownik próbuje wejść na stronę internetową, jeśli IP nie jest zbuforowane w resolwerze DNS, zostanie wystosowane zapytanie do **serwera nazw głównych** (ang. *Root Name Server*) z prośbą o podanie adresu IP **serwera nazw domen najwyższego poziomu** (ang. *Top-Level Domain Name Server*). Domena najwyższego poziomu (ang. *Top Level Domain*, TLD) jest zazwyczaj używana przez właścicieli stron internetowych jako **rejestrator nazw**. Po wysłaniu ostatecznego zapytania o adres IP **domeny drugiego poziomu** użytkownik będzie mógł uzyskać dostęp do strony internetowej. Na rysunku 3.14 znajduje się przykład użytkownika próbującego odwiedzić stronę internetową Wikipedii.




**Rysunek 3.14.** Przykład protokołu DNS

## Sieci bezprzewodowe

**Wi-Fi** (ang. *Wireless Fidelity*) to technologia wykorzystująca fale radiowe do przesyłania danych z sieci do urządzeń sieciowych. Brak przewodów sprawia, że jest to bardzo wygodne rozwiązanie dla użytkowników, a jego zastosowanie zostało szeroko rozpowszechnione na całym świecie. Chociaż urządzenia muszą się znajdować w zasięgu sygnału, aby móc połączyć się z siecią, **punkty dostępowe** służą do wzmacniania sygnałów Wi-Fi i zwiększania zasięgu sieci bezprzewodowej.

### Bezpieczeństwo identyfikatora zestawu usług (SSID)

Identyfikator zestawu usług (ang. *Service Set Identifier*, **SSID**) to ogólnie nazwa sieci Wi-Fi. To nazwa, którą wybieramy z listy SSID, gdy chcemy się połączyć z konkretną siecią. W identyfikatorach SSID rozróżniana jest wielkość liter i długość do 32 znaków alfanumerycznych. Informacja o SSID jest dołączana do pakietów sieciowych, gdy informacje są przesyłane przez sieć bezprzewodową. Gwarantuje to, że dane są przesyłane do i z właściwej sieci.

Jeden punkt dostępowy może mieć więcej niż jeden identyfikator SSID. Różne identyfikatory SSID zapewniają użytkownikom dostęp do różnych sieci o różnych regułach i właściwościach.

Jeśli dwie sieci mają ten sam identyfikator SSID, urządzenia sieciowe będą się próbowały połączyć z siecią o najsilniejszym sygnale lub z tą, która zostanie wykryta jako pierwsza. Jeśli w sieci są włączone opcje zabezpieczeń, przed nawiązaniem połączenia zostanie wyświetlona prośba o podanie hasła.

Jeśli sieć nie ma włączonych opcji zabezpieczeń sieci bezprzewodowej, każdy może się z nią połączyć, znając tylko identyfikator SSID. Ponadto sygnały nie są szyfrowane, więc każdy, kto spróbuje je przechwycić, będzie w stanie zrozumieć dane.

## Kanały Wi-Fi

**Kanały Wi-Fi** to nośniki, których sieci bezprzewodowe używają do przesyłania danych. Pasmo częstotliwości 2,4 GHz ma 11 kanałów i lepszy zasięg, natomiast pasmo częstotliwości 5 GHz ma 45 kanałów i większą szybkość. Jeśli router nie jest dwupasmowy, będzie korzystać z jednego z tych dwóch pasm częstotliwości. Ponieważ liczba dostępnych kanałów jest ograniczona, możemy napotkać zakłócenia. Zdarza się, że duża liczba urządzeń korzysta z tego samego kanału. Gdy kanał jest zatłoczony, zwiększa się czas potrzebny na transmisję. Innym razem kanały nakładają się na siebie, a samo nakładanie się generuje zakłócenia.

Na przykład w paśmie 2,4 GHz każdemu kanałowi przydzielono 2 MHz i jest on oddzielony od innych kanałów o 5 MHz. Ilość miejsca, jaką dysponuje 11 kanałów, wynosi 100 MHz, więc nakładanie się niektórych kanałów jest nieuniknione. Kanały 1, 6 i 11 są kanałami nienakładającymi się. Coś podobnego dzieje się w paśmie częstotliwości 5 GHz, gdzie tylko 25 z 45 kanałów nie nakłada się na siebie; to jest 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161 i 165.

O tym, który kanał będzie używany, decyduje elektronika routera. Kanał, który jest używany, jest zmieniany po każdym ponownym uruchomieniu routera. Można go również zmienić poprzez zmianę ustawień sieci bezprzewodowej w panelu administracyjnym routera.

## Dostęp chroniony Wi-Fi (WPA), WPA2 i WPA3

**Protokół WPA** (ang. *Wi-Fi Protected Access*) [2003] i jego późniejsze wersje, **Wi-Fi Protected Access II** (**WPA2**) [2004] i **Wi-Fi Protected Access 3** (**WPA3**) [2018], to trzy protokoły zabezpieczeń, które zostały opracowane przez Wi-Fi Alliance w celu zabezpieczenia sieci bezprzewodowych w odpowiedzi na problemy z lukami w zabezpieczeniach znalezione w poprzednim systemie. Był on znany pod nazwą Wired Equivalent Privacy (WEP) i został oficjalnie wycofany przez Wi-Fi Alliance w 2004 r.

WAP używał protokołu **Temporal Key Integrity Protocol** (TKIP), który wykorzystuje system klucza przypisanego do pakietu, co poprawiło bezpieczeństwo stałego klucza używanego przez WEP. Chociaż TKIP został zastąpiony przez **Advanced Encryption Standard** (AES), TKIP został opracowany na bazie komponentów pochodzących z WEP, więc przestał być używany, ponieważ również był hakowany przez hakerów. Począwszy od 2006 r., protokół WPA został oficjalnie zastąpiony przez WPA2.

Liczne luki zostały znalezione również w protokole WPA2, w którym pozostawiono protokół TKIP dla zachowania współpracy z protokołem WPA. WPA2 jest podatny na **ataki reinstalacji kluczy** (ang. *Key Reinstallation Attacks*, KRACK) oraz ataki słownikowe.

W WPA3 zaimplementowano nową metodę uzgadniania klucza (ang. *handshake*): **jednoczesne uwierzytelnianie podmiotów równorzędnych** (ang. *Simultaneous Authentication of Equals*, SAE), zwane też **wymianą klucza Dragonfly** (ang. *Dragonfly Key Exchange*). Metoda ta sprawia, że szyfrowanie WPA3 jest odporne na ataki słownikowe, nawet jeśli hasło sieciowe jest słabsze niż zalecane.

W WPA3 zaimplementowano metodę bezpiecznego przesyłania danych (ang. *forward secrecy*). W tym przypadku, nawet jeśli atakujący jest w posiadaniu hasła sieciowego, nie będzie w stanie przechwycić ruchu sieciowego. System **oportunistycznego szyfrowania bezprzewodowego** (ang. *Opportunistic Wireless Encryption*, OWE) wykorzystuje mechanizm wymiany kluczy Diffiego-Hellmana do szyfrowania komunikacji między urządzeniem a routerem, a klucz deszyfrujący jest unikalny dla każdego klienta.

Pomimo tych wszystkich usprawnień bezpieczeństwa w zeszłym roku badacze ujawnili **lukę bezpieczeństwa Dragonblood** (*https://papers.mathyvanhoef.com/dragonblood.pdf*), która pozwala atakującemu na obejście metody uzgadniania klucza (handshake'u) typu Dragonfly.

Teraz, gdy już omówiliśmy wszystkie podstawy sieci, przyjrzyjmy się obsłudze logów w systemie Windows.

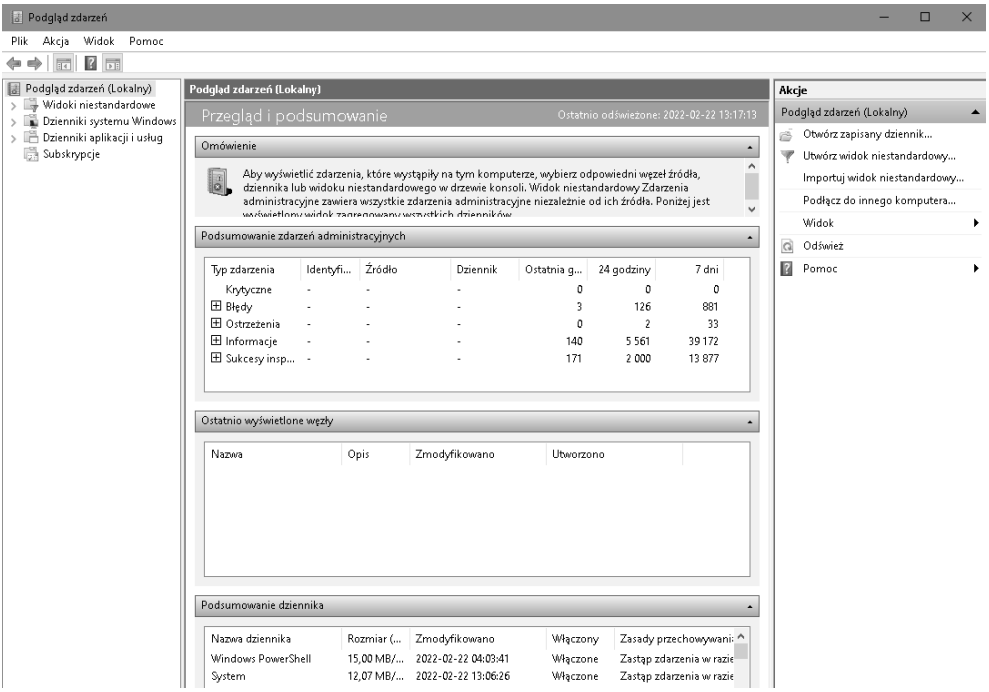
# Narzędzia dostępne w systemie Windows

Prawdopodobnie wiesz już, że Windows jest najczęściej używanym systemem operacyjnym na świecie, więc są szanse, że będziesz miał do czynienia z systemami Windows w swojej organizacji. Na szczęście dla nas Windows posiada kilka natywnych narzędzi przeznaczonych do audytu, które możemy wykorzystać do zbierania informacji o naszym środowisku.

## Podgląd zdarzeń w systemie Windows

Podgląd zdarzeń w systemie Windows (ang. *Windows Event Viewer*) jest natywnym narzędziem Windows, w którym można znaleźć szczegółowe informacje o zdarzeniach generowanych przez aplikacje Windows oraz o innych zdarzeniach zachodzących w systemie. Uruchamia się on automatycznie przy starcie systemu operacyjnego. Niektóre aplikacje instalowane na komputerze korzystają z możliwości dziennika zdarzeń Windows (ang. *Windows Event Log*), podczas gdy inne generują własne dzienniki. Jest to doskonałe narzędzie do rozwiązywania problemów z błędami systemu operacyjnego i aplikacji, a także do poszukiwania zagrożeń.

Dostęp do aplikacji Podgląd zdarzeń można uzyskać poprzez przejście do *Panelu sterowania/System i zabezpieczenia/Narzędzia administracyjne* i wybranie tej właśnie aplikacji. Można również wpisać *Podgląd zdarzeń* w wyszukiwarce systemu Windows lub otworzyć okno dialogowe *Uruchom* (*Windows+R*) i wpisać *eventvwr*. Po wykonaniu tych czynności pojawi się panel pokazany na rysunku 3.15.

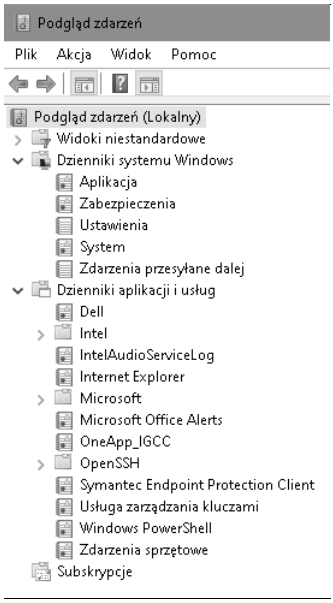



**Rysunek 3.15.** Okno narzędzia Podgląd zdarzeń

Po lewej stronie okna znajduje się panel nawigacyjny, w którym można wybrać różne rodzaje dostępnych dzienników (rysunek 3.16). Dwie główne kategorie to *Dzienniki systemu Windows* oraz *Dzienniki aplikacji i usług*.

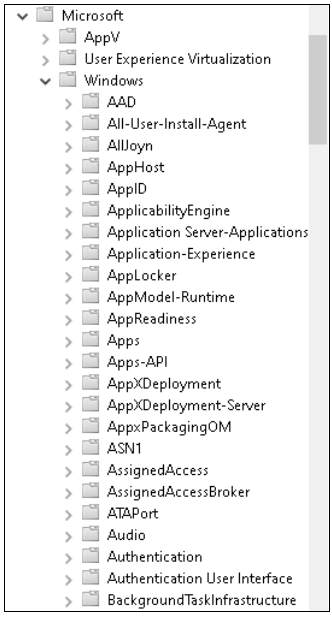
Wśród dzienników systemu Windows rozróżniamy pięć różnych typów:

- **Dzienniki aplikacji**, gdzie dane pochodzą z aplikacji hostowanych na lokalnej maszynie.
- **Dzienniki zabezpieczeń** związane z kontami, logowaniami, audytami i innymi zdarzeniami systemu zabezpieczeń.
- **Dzienniki konfiguracji** zawierające informacje związane z aktualizacjami i uaktualnieniami systemu Windows.
- **Dzienniki systemowe** dla komunikatów generowanych przez system operacyjny.
- **Dzienniki zdarzeń przekazywanych** — komunikaty wysyłane z innych komputerów do abonenta centralnego. Jeśli urządzenie nie pracuje jako centralny abonent, ta część pozostanie pusta.



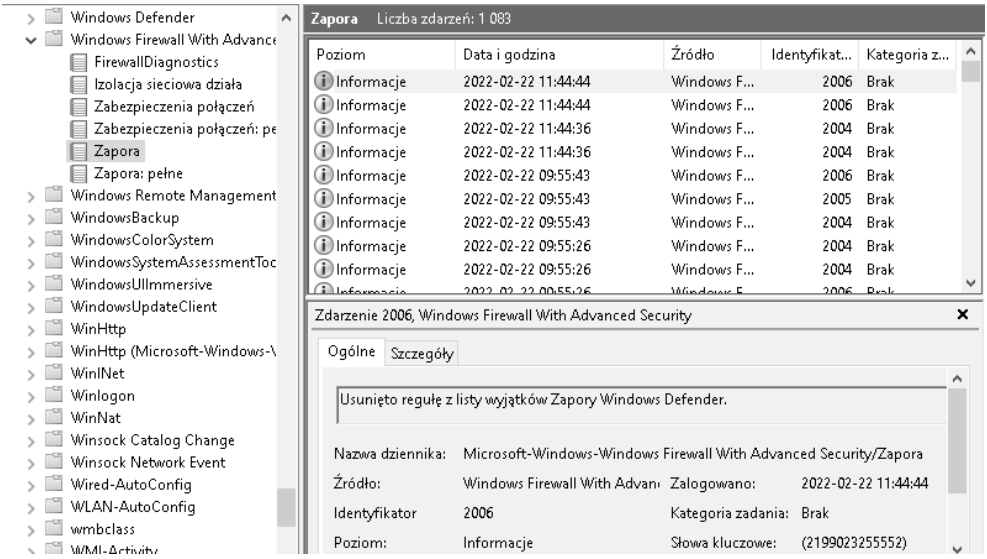

**Rysunek 3.16.** Panel nawigacyjny narzędzia Podgląd zdarzeń

W części *Dzienniki aplikacji i usług* widzimy folder *Microsoft*. Wewnątrz niego znajduje się folder *Windows* zawierający pełną listę aplikacji w kolejności alfabetycznej (rysunek 3.17). Aby zobaczyć dziennik aplikacji, musimy ją wybrać. Wśród nich są między innymi **Zapora Windows Defender** czy **WMI**.




**Rysunek 3.17.** Lista aplikacji systemu Windows

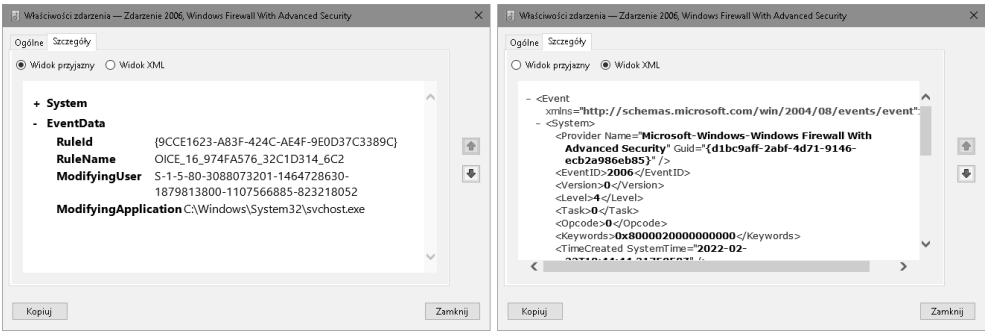
Aby uzyskać dostęp do tych wpisów w dzienniku, wystarczy kliknąć wybraną aplikację w lewym panelu, a pojawi się szczegółowy widok (rysunek 3.18). Aby przeczytać informacje o zdarzeniu w jego własnym oknie, wystarczy to zdarzenie szybko dwukrotnie kliknąć.




**Rysunek 3.18.** Lista zdarzeń aplikacji Zapora systemu Windows

**Przeglądarka zdarzeń** klasyfikuje zdarzenia według pięciu poziomów: krytyczny, błąd, ostrzeżenie, informacyjny i pełny.

Zakładka *Szczegóły* oferuje dwa możliwe widoki zdarzenia — przetworzony do postaci przyjaznej dla użytkownika, który Windows oznaczył jako *Przyjazny*, oraz sformatowany z użyciem XML-a (rysunek 3.19).




**Rysunek 3.19.** Widok szczegółów zdarzenia

## Instrumentacja zarządzania systemem Windows (WMI)

**WMI** (ang. *Windows Management Instrumentation* — instrumentacja zarządzania systemem Windows) to *infrastruktura do zarządzania danymi i operacjami w systemach operacyjnych opartych na Windows*. WMI jest używana do lokalnego i zdalnego dostępu do danych związanych z zarządzaniem z poziomu innych systemów Windows. Zdalne połączenia z WMI są realizowane poprzez **DCOM** (ang. *Distributed Component Object Model*) lub **WinRM** (ang. *Windows Remote Management*).

WMI jest tak potężna, że niektóre źródła zaawansowanych trwałych zagrożeń zaczęły używać jej jako środka do wykonywania poleceń w systemie, którego bezpieczeństwo zostało naruszone, do zbierania informacji, uzyskiwania odporności, a nawet przemieszczania się w sieci pomiędzy komputerami. Jego użycie zostało zdefiniowane jako osobna technika w MITRE ATT&CK™ Framework (*https://attack.mitre.org/techniques/T1047/*).

Aktywność systemu WMI może być śledzona za pomocą aplikacji Podgląd zdarzeń w systemie Windows, ale do szczegółowego monitorowania aktywności WMI zalecane jest użycie aplikacji **Śledzenie zdarzeń dla Windows** (ETW).

## Śledzenie zdarzeń dla Windows (ETW)

**Śledzenie zdarzeń dla Windows** (ang. *Event Tracing for Windows*, ETW) jest funkcjonalnością pozwalającą na debugowanie i diagnostykę systemu Windows, która zapewnia *efektywne śledzenie na poziomie jądra, co pozwala na rejestrowanie zdarzeń zdefiniowanych przez jądro lub aplikację do pliku dziennika*. ETW pozwala na śledzenie zdarzeń w środowisku produkcyjnym bez ponownego uruchamiania komputera lub aplikacji.

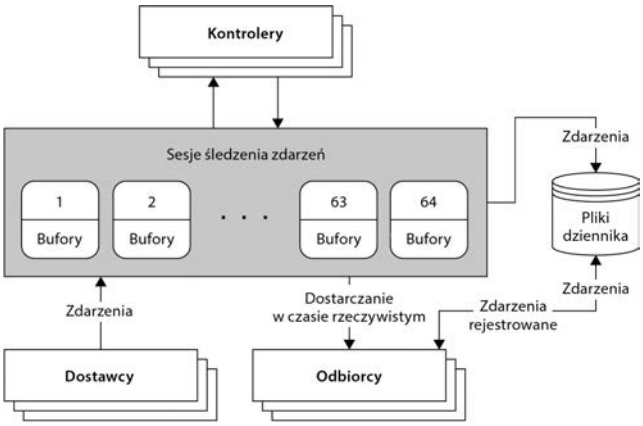
Według dokumentacji Microsoftu API śledzenia zdarzeń jest podzielone na trzy komponenty:

- **kontrolery** zdarzeń (uruchamiają i zatrzymują sesje śledzenia oraz włączają dostawców),
- **dostawcy** zdarzeń,
- **odbiorcy** zdarzeń.

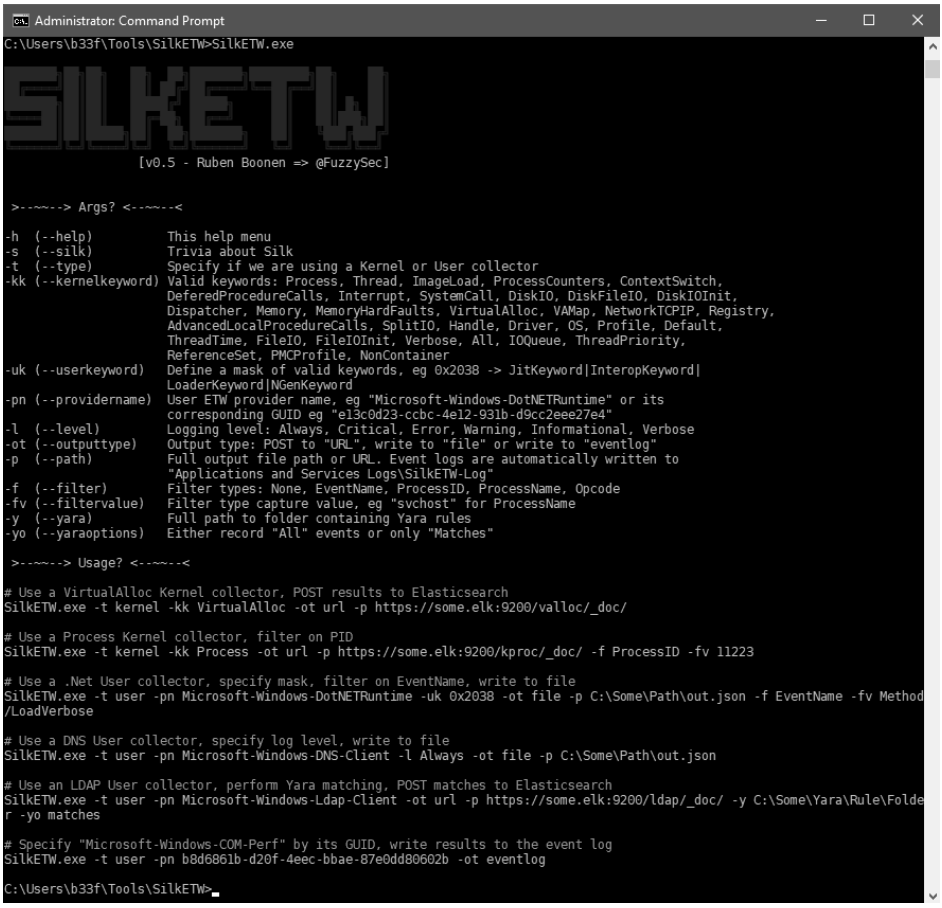
Rysunek 3.20 przedstawia śledzenie zdarzeń dla architektury Windows.

Oprócz możliwości debugowania i diagnostyki ETW dostarcza metryki i dane, które są przydatne do wykrywania i badania aktywności podmiotów stwarzających zagrożenie, choć nie są one zbyt łatwe do zebrania.

Ruben Boonen opracował narzędzie o nazwie SilkETW (rysunek 3.21), które stara się pomóc w tym procesie i pozwala na pobieranie danych ETW w formacie JSON. Dzięki temu można łatwo zintegrować pozyskane dane z systemami SIEM innych firm, takimi jak Elasticsearch czy Splunk. Dodatkowo JSON może zostać przekonwertowany i wyeksportowany do PowerShella, a Ty możesz połączyć Yara Rules z SilkETW, aby rozszerzyć możliwości swoich badań nad bezpieczeństwem.




**Rysunek 3.20.** Schemat funkcji śledzenia zdarzeń w systemie Windows (ETW)




**Rysunek 3.21.** Interfejs aplikacji SilkETW

Możesz pobrać SilkETW i przeczytać o nim więcej, przechodząc do jego oficjalnego repozytorium GitHub pod adresem *https://github.com/fireeye/SilkETW*.

# Źródła danych

Możemy rozróżnić trzy rodzaje źródeł danych: **źródła danych punktów końcowych**, **źródła danych sieciowych** oraz **źródła danych bezpieczeństwa**. Każde źródło danych zapewnia dzienniki aktywności. Plik dziennika jest zapisem zdarzeń, które miały miejsce w określonym środowisku lub podczas wykonywania oprogramowania. Dzienniki składają się z wpisów, gdzie każdy wpis odpowiada zdarzeniu.

Mimo że dzienniki są bardzo użytecznym źródłem informacji podczas monitoringu i analizy śledczej, praca z nimi wiąże się z wieloma problemami dotyczącymi różnych formatów i pojemności pamięci. Poradnik *Guide to Computer Security Log Management* (*https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf*), napisany przez Karen Kent i Murugiaha Souppayę, oferuje dobry wgląd w najczęstsze problemy i sposoby ich rozwiązywania.

Większość przykładów, które zobaczysz w kolejnych rozdziałach, została zebrana z przeglądarki dziennika zdarzeń systemu Windows. Byłoby świetną wprawką, gdybyś podczas czytania tej części otworzył przeglądarkę dziennika zdarzeń i spróbował znaleźć podobne przykłady.

Kluczem do zrozumienia i umiejętności analizowania logów jest po prostu zapoznanie się z nimi poprzez regularne, a nawet codzienne ich przeglądanie. Logi zmieniają swoją zawartość i format, co utrudnia ich zrozumienie osobie, która z nimi pracuje. Trudność ta zwiększa się wraz z wielkością organizacji, wzrostem systemów i aplikacji oraz ograniczeniem dostępnych zasobów. Częste i ciągłe przeglądanie danych pozwoli na lepsze ich zrozumienie, a także na rozpoznanie czegoś, co przełamuje schemat. W tym rozdziale omówimy różne rodzaje źródeł danych, które możemy wykorzystać.

## Dane z punktów końcowych

Używając terminu „punkt końcowy”, rozumiemy przez to, że jest to każde urządzenie, które znajduje się w „punkcie końcowym” sieci. Zazwyczaj termin ten jest używany w odniesieniu do komputerów (zarówno laptopów, jak i desktopów) oraz urządzeń mobilnych, ale termin ten dotyczy również serwerów czy urządzeń „internetu rzeczy” (IoT).

### Dzienniki systemowe

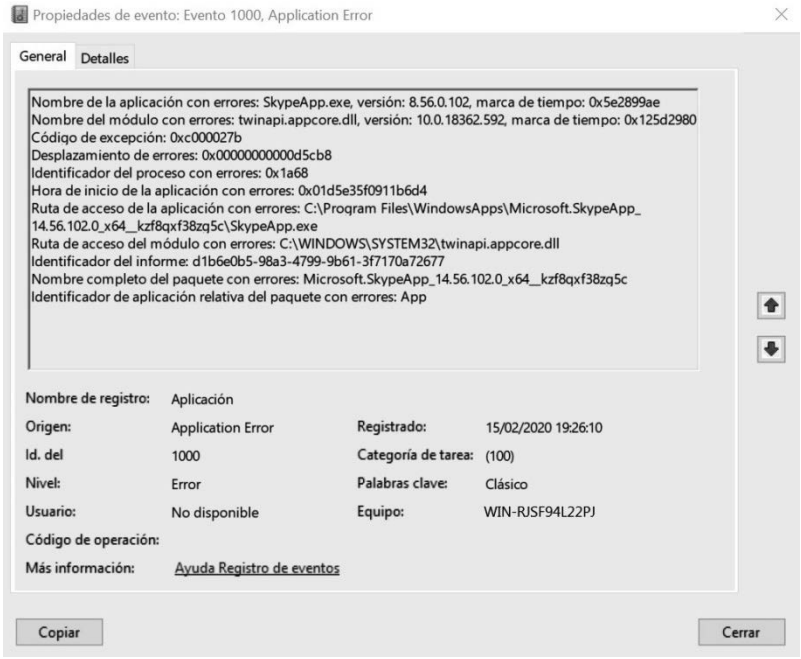
Dzienniki systemowe odnoszą się do plików dziennika, w których zapisywane są zdarzenia systemowe generowane przez komponenty systemu operacyjnego. Informacje w nich zawarte mogą być różne — od zmian w systemie, błędów i aktualizacji po zmiany w urządzeniach, uruchamianie usług, zamykanie systemu i inne.

## Dzienniki aplikacji

**Aplikacja** to dowolny element oprogramowania komputerowego zaprojektowany tak, aby pomóc użytkownikowi w wykonywaniu czynności, takich jak kodowanie, pisanie, edycja zdjęć itp. Istnieje wiele rodzajów aplikacji i wielu ich twórców. W konsekwencji dzienniki aplikacji mogą się bardzo różnić — nie tylko pod względem formatowania, ale także pod względem rodzaju rejestrowanych informacji. Niektóre aplikacje będą miały własne systemy rejestrowania zdarzeń, podczas gdy inne będą korzystać z możliwości logowania systemu operacyjnego. Poradnik *Guide to Computer Security Log Management* (poradnik zarządzania logami bezpieczeństwa komputerowego) identyfikuje cztery typy rejestrowanych informacji, które zazwyczaj są w nich uwzględniane:

- **informacje o użytkowaniu** (na przykład kiedy wystąpiło zdarzenie, co to było, rozmiar pliku itd.),
- **żądania klientów i odpowiedzi serwerów** (na przykład gdy przeglądarka po stronie klienta wykonuje żądania HTTPS do serwera WWW),
- **informacje o kontach** (takie jak próby uwierzytelnienia lub wykonywanie uprawnień użytkownika, zmiany w kontach użytkowników itd.),
- **działania operacyjne** (takie jak wyłączenia, zmiany konfiguracji, błędy i ostrzeżenia).

Na rysunku 3.22 znajduje się przykład błędu aplikacji Skype, który zawiera niektóre z tych informacji.




**Rysunek 3.22.** Przykład błędu wygenerowanego przez aplikację Skype

Teraz przyjrzyjmy się logom PowerShella.

## Dzienniki PowerShell

Coraz więcej złośliwego oprogramowania wykorzystuje PowerShell do wykonywania komend na komputerach ofiar. PowerShell jest naprawdę potężnym środowiskiem poleceń i językiem skryptowym dla systemu Windows. Obecnie Windows 10 posiada domyślnie włączoną rozszerzoną możliwość tworzenia i przeglądania dzienników PowerShell, ale poprzednie wersje systemu Windows wymagały ręcznego aktywowania tej możliwości poprzez aktualizacje oprogramowania. Użytkownicy Windows Server 2012 i poprzednich wersji borykali się z tym samym problemem.

Ta rozszerzona możliwość pozwala nam zobaczyć, jakie polecenia i skrypty zostały wykonane za pomocą PowerShella (rysunek 3.23).


**Rysunek 3.23.** Wykonany skrypt aplikacji PowerShell — przykład zapisów dziennika

Oprócz tego PowerShell może być bardzo przydatny do pracy z dziennikami zdarzeń i śledzenia tego, co zostało zrobione na komputerze. Przemysław Kłys napisał naprawdę przydatny przewodnik zawierający kilka wartych wypróbowania poleceń, które można znaleźć w dwóch artykułach, zatytułowanych *Everything you wanted to know about Event Logs and then some* (*https://evotec.xyz/powershell-everything-you-wanted-to-know-about-event-logs/*) oraz *The only PowerShell command you will ever need to find out who did what in Active Directory* (*https://evotec.xyz/the-only-powershell-command-you-will-ever-need-to-find-out-who-↪did-what-in-active-directory/*). Oczywiście, zawsze możesz zapoznać się z oficjalną dokumentacją Windows PowerShell: *https://docs.microsoft.com/en-us/powershell/?view=powershell-5.1*.

## Dzienniki Sysmon

Jeśli śledzisz ostatnio wiadomości na temat łowców zagrożeń, mogłeś zauważyć, że **Sysmon** wydaje się powszechnym ulubieńcem. **Monitoring systemu** (ang. *System Monitoring*, Sysmon) jest częścią pakietu Sysinternals Suite Marka Russinovicha (*https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite*). Powodem, dla którego zdobył on taką popularność, jest to, że okazał się świetnym sposobem na uzyskanie wglądu w punkty końcowe bez wpływu na wydajność systemu.

Sysmon jest usługą systemową i sterownikiem urządzenia, który monitoruje i rejestruje aktywność systemową w dzienniku zdarzeń Windowsa. Konfiguracja Sysmona może być dostosowana do naszych potrzeb, ponieważ dostarcza on reguł XML, które mogą włączać i wyłączać nieinteresujące nas elementy. Lista dostępnych opcji filtrowania zwiększa się wraz z każdą aktualizacją Sysmona.

Sysmon dostarcza informacje o tworzeniu procesów, tworzeniu i modyfikacji plików, połączeniach sieciowych, tworzeniu procesów i ładowaniu sterowników lub bibliotek DLL, wśród innych naprawdę ciekawych funkcji, takich jak możliwość generowania hashy dla wszystkich plików binarnych działających w systemie.

Instalacja aplikacji Sysmon jest dość prosta — wystarczy pobrać plik wykonywalny Sysmon z *https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon* i uruchomić jedno z poniższych poleceń dla domyślnej instalacji, w zależności od wersji systemu operacyjnego:

```
c:\> sysmon64.exe –i
c:\> sysmon.exe -i
```

Poniżej znajduje się przykład informacji wyjściowych, które Sysmon wyświetli po uruchomieniu CMD:

```
Process Create:
RuleName:
UtcTime: 2020-02-17 21:16:05.208
ProcessGuid: {dc035c9e-0295-5e4b-0000-001007ecc80a}
ProcessId: 635140
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.18362.449 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: "C:\WINDOWS\system32\cmd.exe"
CurrentDirectory: C:\Users\pc\
User: WIN-RJSF94L22PJ
LogonGuid: {dc035c9e-dd69-5e46-0000-002082200900}
LogonId: 0x92082
TerminalSessionId: 1
IntegrityLevel: Medium
```

```
Hashes: SHA1=8DCA9749CD48D286950E7A9FA1088C937CBCCAD4
ParentProcessGuid: {dc035c9e-dd6a-5e46-0000-0010e8600a00}
ParentProcessId: 7384
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\WINDOWS\Explorer.EXE
```

### Monitorowanie integralności plików i rejestrów

**Monitorowanie integralności plików i rejestrów** (ang. *File and Registry Integrity Monitoring*, FIM) odnosi się do praktyki polegającej na próbach wykrywania zmian w plikach lub rejestrach poprzez porównywanie ich z poziomem odniesienia. Jest to zwykle wykonywane za pomocą rozwiązań zabezpieczających innych firm, które ostrzegają użytkownika o zmianach w określonych plikach, katalogach lub rejestrach.

Jeśli nie jest to zrobione prawidłowo, FIM w roli mechanizmu kontroli bezpieczeństwa może się okazać nieskuteczny i generować dużo „szumu", ponieważ należy się spodziewać, że pliki w systemie operacyjnym będą się w pewnym stopniu zmieniać. Dlatego konieczne jest zapewnienie niezbędnego kontekstu dla tych zmian, aby FIM był skuteczny.

### Serwery plików

Audyt serwerów plików jest przydatnym mechanizmem służącym do śledzenia, kto ma dostęp do plików organizacji. Windows Server ma wbudowane zasady audytu o nazwie **Kontrola dostępu do obiektów** (ang. *Audit Object Access*). Po określeniu, które pliki lub katalogi mają być monitorowane, dostęp do nich będzie widoczny poprzez aplikację Podgląd zdarzeń w systemie Windows.

Funkcja ta jest szczególnie przydatna, jeśli Ty lub Twoja organizacja padliście ofiarą cyberataku i musicie śledzić pliki, które mogły zostać udostępnione, zmienione lub nawet skradzione.

Istnieje kilka przewodników, które mówią, jak włączyć tę funkcję; jeden, który w prosty sposób opisuje każdy krok, można znaleźć na *https://www.varonis.com/blog/windows-file-*
*↪system-auditing/*.

## Dane sieciowe

Przyjrzyjmy się źródłom danych, które możemy zebrać od strony sieci.

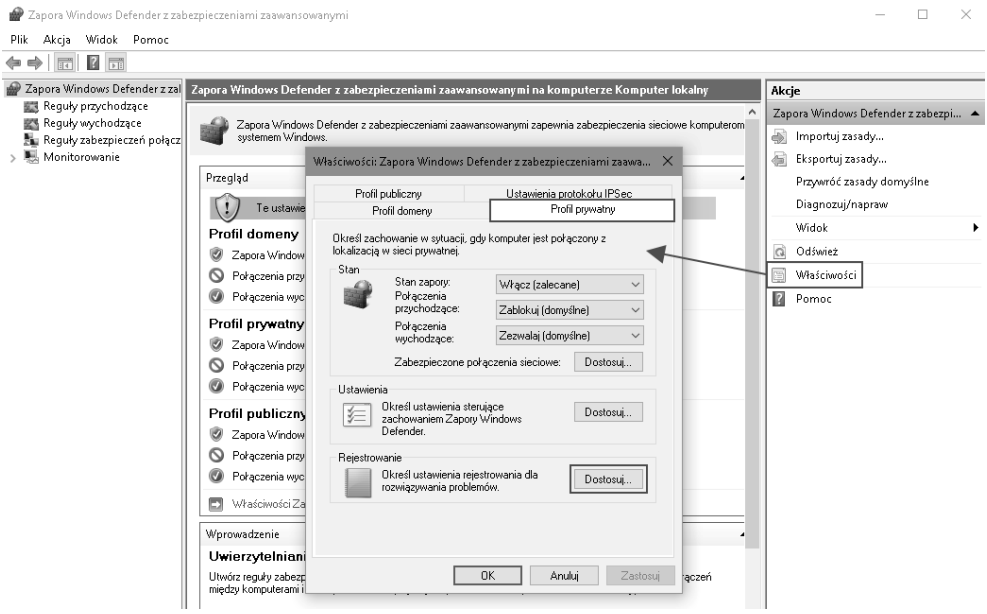
### Dzienniki aplikacji Zapora Windows Defender

Jak wspomnieliśmy wcześniej, zapora jest systemem bezpieczeństwa sieciowego, który monitoruje ruch przychodzący i wychodzący. Skuteczność zapory opiera się zazwyczaj na regułach mówiących jej, które połączenia blokować. Zapory sieciowe działają pomiędzy dwoma sieciami lub większą ich liczbą, natomiast zapory oparte na hostach działają na komputerach.

Zapora sprawdza, na jaki adres następuje połączenie, skąd pochodzi i na jaki port jest kierowane. Korzystając ze skonfigurowanego zestawu reguł, zapora określa, czy połączenie może być zaufane, czy też je zablokuje.

Jedną z ważnych cech dzienników zapory jest to, że możemy je wykorzystać do identyfikacji złośliwej aktywności w naszej sieci, sprawdzenia, czy nie dochodzi do połączeń wychodzących, które nie powinny mieć miejsca, a nawet sprawdzenia, czy nie dochodzi do prób dostępu do zapory lub innych zaawansowanych systemów w obrębie organizacji. Dzienniki zapory mogą również pomóc zespołom ds. reagowania na incydenty zrozumieć, w jaki sposób zagrożenie bezpieczeństwa zdołało ominąć zaporę.

Zapora wbudowana w system Windows firmy Microsoft domyślnie nie rejestruje żadnego ruchu. Aby ją aktywować, należy przejść do okna *Właściwości* zapory Windows Defender i w wyświetlonym oknie wybrać zakładkę *Profil prywatny*, a następnie kliknąć przycisk *Dostosuj* w sekcji *Rejestrowanie*, jak pokazano na rysunku 3.24.

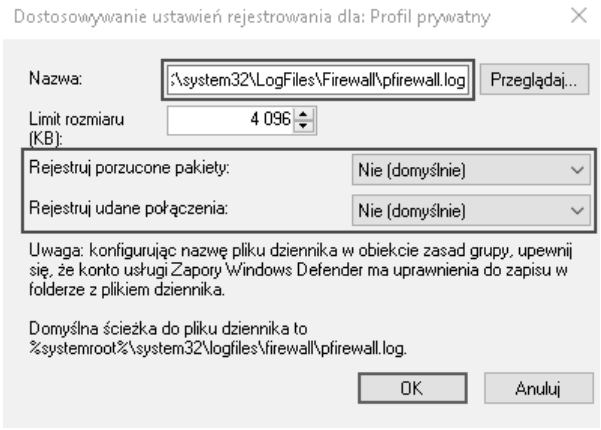



**Rysunek 3.24.** Okno właściwości aplikacji Zapora Windows Defender

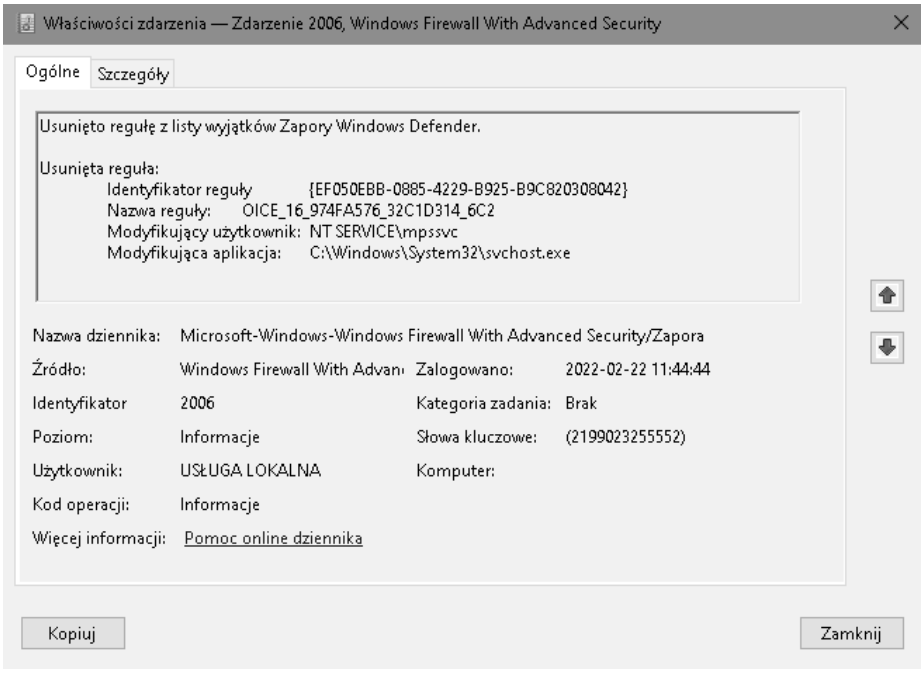
Spowoduje to otwarcie okna *Dostosowywanie ustawień rejestrowania*, w którym można zmienić wartość domyślną i rejestrować porzucone pakiety, udane połączenia oraz lokalizację i nazwę pliku dziennika. Widać to na zrzucie ekranu przedstawionym na rysunku 3.25.

Na rysunku 3.26 znajduje się przykład dziennika aplikacji Zapora Windows Defender.

Ważne jest, aby analizować dzienniki zapory, gdyż to pozwala zrozumieć, co jest normalną aktywnością, a co może być odstępstwem od normy. Niektórymi przyczynami odstępstw od normy mogą być modyfikacje konfiguracji zapory, porzucony ruch, zakłócenia w działaniu zapory, użycie podejrzanych portów oraz inne przyczyny.




**Rysunek 3.25.** Okno ustawień dziennika




**Rysunek 3.26.** Przykład dziennika aplikacji Zapora Windows Defender

Oczywiście, zapory różnych producentów będą miały różne formaty działania. Poniżej znajduje się przykład dziennika zapory CISCO ASA:

```
Feb 18 2020 01:07:57: %ASA-4-107089: Deny tcp src dmz:X.X.X.62/44329 dst
↪outside:X.X.X.6/23 by access-group "ops_ dmz" [0xa4eab611, 0x0]
```

## Routery/przełączniki

Ponieważ zadaniem routerów i przełączników jest kierowanie ruchem w sieci, ich dzienniki dostarczają informacji na temat aktywności sieci. Taka możliwość jest przydatna dla celów monitorowania, które miejsca są odwiedzane, ponieważ może to pomóc w wykryciu złośliwej aktywności. Zazwyczaj opcja ta nie jest domyślnie włączona i musi być ręcznie wprowadzona z poziomu panelu konfiguracyjnego routera.

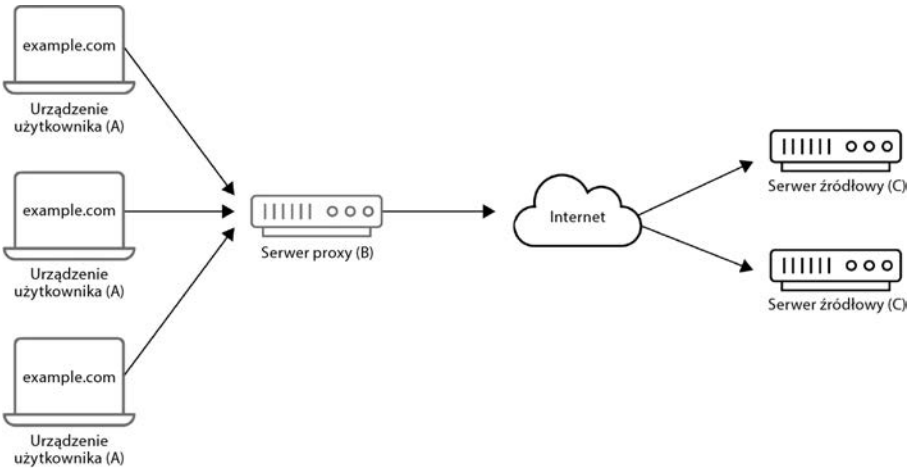
Monitorowana aktywność routera napotyka na dwa główne problemy:

- Codziennie przez routery przechodzą ogromne ilości ruchu.
- Prywatność. Przede wszystkim zbieranie danych dotyczących aktywności przeglądania stron internetowych przez konkretnego użytkownika jest naruszeniem jego prywatności. Regulacje i możliwości dotyczące tego aspektu różnią się w poszczególnych krajach, dlatego przed podjęciem tego typu działań należy sprawdzić, jakie konsekwencje mogą one mieć zarówno dla użytkownika, jak i dla organizacji.

> Aby uzyskać więcej informacji na ten temat, zapoznaj się z artykułami poświęconymi tej tematyce: *Is it Unlawful to Collect or Store TCP/IP Log Data for Security Purposes?* Marka Rascha (*https://securityboulevard.com/2018/09/is-it-unlawful-to-collect-or-store-↪tcp-ip-log-data-for-security-purposes/*) oraz *Why You Need to Include Log Data in your Privacy Policy* Jaclyn Kilani (*https://www.termsfeed.com/blog/privacy-policy-log-data/*).

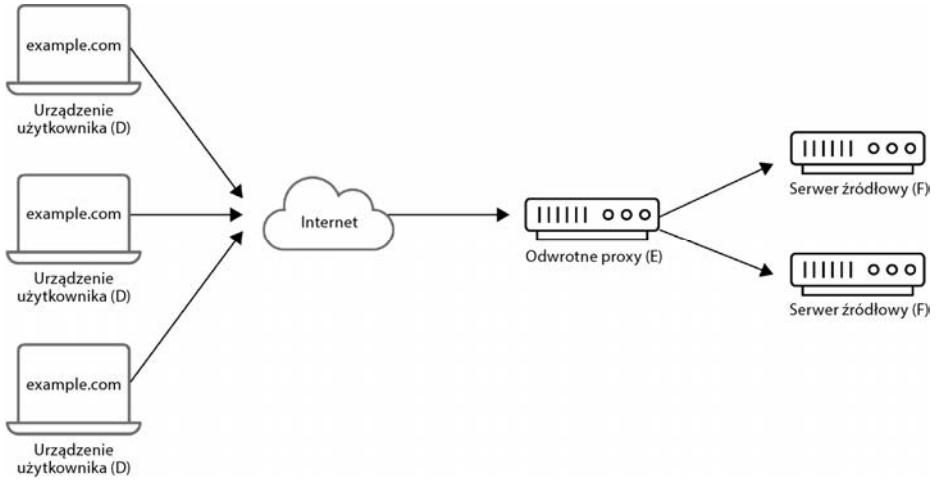
## Serwery proxy, odwrotne serwery proxy i równoważenie obciążenia

Każdy serwer działający jako pośrednik pomiędzy zestawem komputerów a internetem jest nazywany **serwerem proxy** (również *forward proxy* lub po prostu *proxy*). Serwer proxy przechwytuje żądanie komputera i komunikuje się z serwerami WWW w ich imieniu (rysunek 3.27). Zamiast adresu IP klienta serwer internetowy otrzyma adres IP serwera proxy. Serwer proxy nie szyfruje ruchu i może jedynie przekierowywać ruch pochodzący z aplikacji z nim powiązanej.




**Rysunek 3.27.** Schemat serwera proxy

**Odwrotny serwer proxy** znajduje się przed serwerem WWW zamiast klienta. Serwer proxy działa jako klient dla serwera WWW i wysyła odpowiedź do oryginalnego klienta (rysunek 3.28).




**Rysunek 3.28.** Schemat odwrotnego serwera proxy

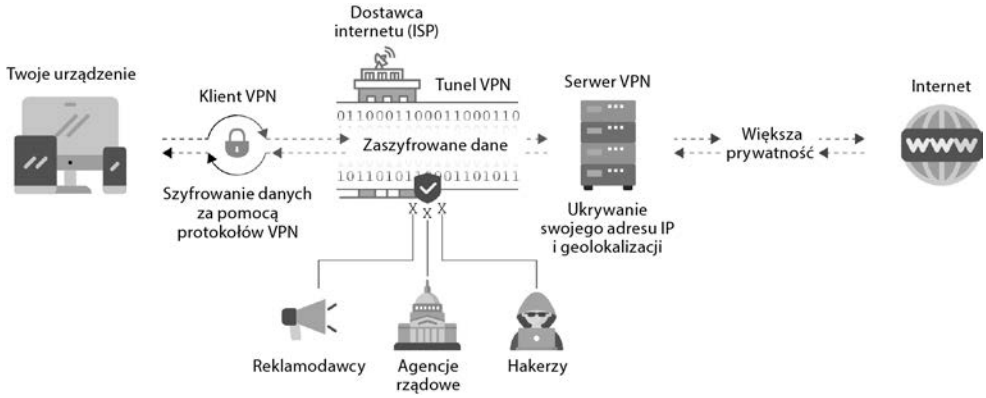
Odwrotne serwery proxy są przydatne w zachowaniu bezpieczeństwa, ponieważ ukrywają adresy IP serwerów internetowych. Mogą być również przydatne przy równoważeniu obciążenia w przypadku witryn o dużym natężeniu ruchu, który musi być rozprowadzany do puli różnych serwerów. Następnie wszystkie żądania są obsługiwane przez odwrotny serwer proxy. Wreszcie, w tym samym czasie odwrotny serwer proxy może pomóc poprawić wydajność poprzez buforowanie.

Biorąc pod uwagę ich funkcjonalność, serwery proxy zawierają żądania, które zostały wykonane przez klienty w sieci organizacji. Większość organizacji biznesowych wdraża **proxy transparentne**. Transparentny proxy to serwer proxy, który jest używany do monitorowania lub blokowania dostępu do określonych stron internetowych.

## Systemy VPN

Podobnie jak serwer proxy, klient **wirtualnej sieci prywatnej** (VPN) również przekierowuje ruch do serwera VPN, ukrywając w ten sposób IP klienta przed serwerem webowym. VPN przekierowuje jednak cały ruch wychodzący od klienta, bez względu na to, która aplikacja wysyła żądanie. Ponadto klient VPN szyfruje cały ruch, aby nikt, kto węszy w Twojej sieci, nie mógł zrozumieć jego treści. Serwer VPN odszyfrowuje zaszyfrowany ruch i wysyła żądanie do internetu (rysunek 3.29).

Niektórzy mogliby powiedzieć, że jeśli głównym powodem korzystania z VPN jest uniknięcie wścibstwa, rejestrowanie w dziennikach ruchu w sieci może się wydawać sprzeczne z intuicją. Istnieją jednak pewne ważne powody, aby utrzymywać pewien rodzaj rejestrowania. Na przykład organizacja może korzystać z systemu VPN, aby zapewnić pracownikom pracującym zdalnie bezpieczny dostęp do sieci firmowej. Nie oznacza to jednak, że traci ona zainteresowanie upewnieniem się, że tylko autoryzowany personel ma dostęp do sieci organizacji poprzez VPN.




**Rysunek 3.29.** Schemat wirtualnej sieci prywatnej VPN

## Serwery webowe WWW

Dziennik serwera webowego WWW jest plikiem tekstowym zapisującym aktywność, która ma miejsce na serwerze.

Poniżej znajduje się przykład naprawdę prostej aplikacji Flask:

```
* Serving Flask app "example.py" (lazy loading)
  * Environment: development
  * Debug mode: on
  * Running on http://127.0.0.1:5000/ (Press CTRL+C to quit)
  * Restarting with stat
  * Debugger is active!
  * Debugger PIN: 237-512-749
PATH: hello_world
127.0.0.1 - - [18/Feb/2020 03:33:23] "GET /api/example/hello_ world HTTP/1.1" 200 -
127.0.0.1 - - [18/Feb/2020 03:42:07] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [18/Feb/2020 03:42:39] "GET /bye_world HTTP/1.1" 404 -
```

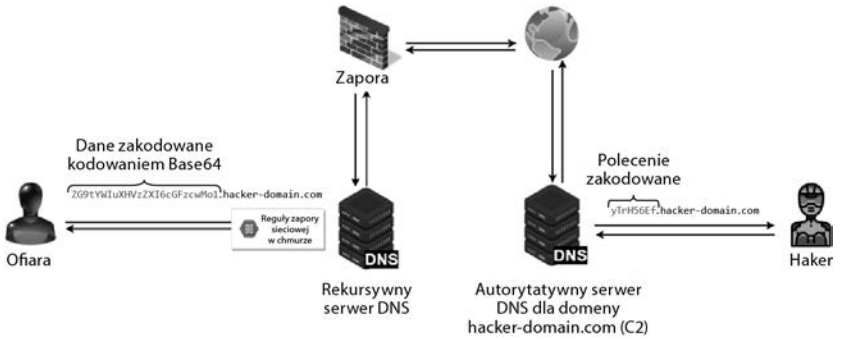
Każda linia w dzienniku reprezentuje żądanie klienta. Na przykład linia **`127.0.0.1 - - [18/Feb/2020 03:33:23] "GET /api/example/hello_world HTTP/1.1" 200 -`** oznacza, że żądanie HTTP `GET` (*http://127.0.0.1:5000/api/example/hello_word*) zostało wykonane 18 lutego 2020 r. o 03:33:23. Kod statusu `200` oznacza, że żądanie zakończyło się sukcesem. W ostatnim wierszu kod statusu `404` oznacza, że strona nie została odnaleziona na serwerze.

Informacje, które może przechowywać dziennik serwera WWW, mogą się różnić w zależności od używanej aplikacji, jej złożoności i, oczywiście, niestandardowych konfiguracji programistycznych. Niektóre z najczęściej dostępnych pól informacyjnych to: data i czas, metoda żądania, agent użytkownika, nazwa usługi i serwera, rozmiar żądanego pliku, adres IP klienta i tak dalej.

Ten typ dziennika może być naprawdę przydatny do identyfikacji złośliwej aktywności próbującej nadużyć aplikacji.

## Serwery DNS

Protokół **DNS** jest praktyczną współzależnością pozwalającą na funkcjonowanie większości innych usług sieciowych. Ponieważ musi on być dostępny, staje się użyteczny dla atakujących w celu wprowadzania złośliwego oprogramowania, wysyłania komend do wykonania na maszynie ofiary lub pozyskiwania informacji. Jest to jeden z powodów, dla których rejestrowanie i monitorowanie ruchu DNS jest tak ważne. Na rysunku 3.30 znajduje się przykładowy schemat pokazujący, jak może przebiegać tego typu komunikacja tunelowa DNS.




**Rysunek 3.30.** Schemat tunelowania DNS

Zapisywanie w dziennikach aktywności systemu DNS w systemie Windows może być aktywowane z poziomu aplikacji Podgląd zdarzeń. Aby aktywować zapisywanie, należy w tej aplikacji w drzewie konsoli przejść do gałęzi *Dzienniki aplikacji i usług/Microsoft/Windows/DNS Client Events/Operacyjny*. Gdy już wejdziesz w to miejsce w drzewku, otwórz prawym przyciskiem myszy menu podręczne i z listy wybierz opcję *Włącz dziennik*. Poniżej znajduje się przykład dziennika zdarzeń usługi DNS:

```
- System
  - Provider
  [ Name]   Microsoft-Windows-DNS-Client
  [ Guid]   {1c95126e-7eea-49a9-a3fe-a378b03ddb4d}
  EventID 3020
  Version 0
  Level 4
  Task 0
  Opcode 0
  Keywords 0x8000000000000000

- TimeCreated
  [ SystemTime] 2020-02-18T07:29:50.674872100Z
  EventRecordID 344
  Correlation

- Execution
  [ ProcessID]  2400
  [ ThreadID]   770488
  Channel Microsoft-Windows-DNS-Client/Operational
  Computer WIN-RJSF94L22PJ
```

```
- Security
  [ UserID]   S-1-5-20

- EventData
  QueryName www.google.com.ar
  QueryType 1
  NetworkIndex 0
  InterfaceIndex 0
  Status 0
  QueryResults 216.58.222.35;
```

# Dane zabezpieczeń

Usługa **podsystemu lokalnej administracji zabezpieczeń** (ang. *Local Security Authority Subsystem Service*, LSASS) zapisuje zdarzenia w oknie **Dziennika zabezpieczeń**, które jest dostępne w aplikacji Podgląd zdarzeń w systemie Windows. Jest on używany głównie do rozwiązywania problemów i badania nieautoryzowanej aktywności. Dziennik ten oraz jego zasady audytu są głównym celem podmiotów stwarzających zagrożenia, próbujących ukryć swoje złośliwe działania.

## Dzienniki Active Directory

Usługa **Active Directory** (AD) stanowi integralną część wszystkich systemów operacyjnych Windows Server. Jest to **kontroler domeny** w **sieciach domenowych systemu Windows**. W sieciach domenowych Windows wszystkie konta i urządzenia są rejestrowane w bazie danych kontrolera domeny. Zasadniczo kontroler domeny jest serwerem (lub grupą serwerów) z uruchomioną usługą Active Directory, zarządzającym dostępem klientów do informacji w katalogach. Kontroler domeny jest odpowiedzialny za uwierzytelnianie wszystkich urządzeń i użytkowników w sieci, instalowanie aktualizacji oprogramowania i egzekwowanie zasad bezpieczeństwa. Protokół **LDAP** (ang. *Lightweight Directory Access Protocol*) jest protokołem, który kontroluje dostęp do katalogów internetowych w usłudze domenowej Active Directory.

Nadużycia w Active Directory są dokonywane przez podmioty stwarzające zagrożenie w celu ominięcia mechanizmów obronnych, podniesienia poziomu uprawnień lub uzyskania dostępu do danych uwierzytelniających. Rejestrowanie aktywności Active Directory pozwala na większą widoczność tego, kto co zrobił. Przy odpowiedniej konfiguracji (*https://community.spiceworks.com/how_to/166859-view-ad-logs-in-event-viewer*) możesz zobaczyć aktywność Active Directory w przeglądarce dziennika zdarzeń systemu Windows.

## Dzienniki Kerberos

W systemie Windows protokół **Kerberos** jest również obsługiwany przez Active Directory, a gdy system Windows otrzyma dane uwierzytelniające, sprawdzi je w katalogu LDAP przed bezpośrednim wydaniem biletu uwierzytelniającego Kerberos. W systemach Linux ten krok „wstępnego uwierzytelniania" jest pomijany.

Protokół Kerberos jest odmianą protokołu pojedynczego logowania, który pozwala użytkownikowi zalogować się przy użyciu nazwy użytkownika i hasła, aby uzyskać dostęp do kilku powiązanych systemów. Kerberos generuje zaszyfrowany bilet uwierzytelniający, który będzie używany do przyznawania użytkownikom dostępu do systemu. Uwierzytelnianie systemu Kerberos sprawdza zdolność klienta do odszyfrowania klucza sesji, który został wysłany wraz z biletem. Jeśli jest to legalna próba dostępu, klient otrzyma klucz sesji i uzyska dostęp do systemu. Następnie klient może zapisać bilet, aby uzyskać dostęp do innych aplikacji w systemie bez konieczności ponownego logowania.

W systemie Windows logi Kerberosa można przeglądać za pomocą przeglądarki dziennika zdarzeń systemu Windows:

```
Success

A Kerberos authentication ticket (TGT) was requested.

Account Information:

  Account Name: Administrator
  Supplied Realm Name: trial-th
  User ID: ACME-FR\administrator

Service Information:

  Service Name: krbtgt
  Service ID: TRIAL-TH\krbtgt

Network Information:

  Client Address: 10.25.14.02
  Client Port: 0

Additional Information:

  Ticket Options: 0x20462231
  Result Code: 0x0
  Ticket Encryption Type: 0x12
  Pre-Authentication Type: 2

Certificate Information:

  Certificate Issuer Name:
  Certificate Serial Number:
  Certificate Thumbprint:

Certificate information is only provided if a certificate was used for pre-
↪authentication.

Pre-authentication types, ticket options, encryption types and result codes are
↪defined in RFC 4120.
```

Następnie omówimy **zarządzanie tożsamością i dostępem** (IAM).

## IAM — zarządzanie tożsamością i dostępem

Celem **IAM** (ang. *Identity and Access Management*) jest zapewnienie, że każdy użytkownik ma dostęp do właściwych zasobów lub są mu one odbierane, gdy jest to wymagane. Chodzi o ustawienie ról i przywilejów dostępu, które uniemożliwiają użytkownikowi uzyskanie większego dostępu, niż wymaga tego jego rola w organizacji.

Systemy IAM są wprowadzane, aby pomóc w modyfikacji i monitorowaniu tych uprawnień. Prawidłowe wdrożenie IAM może stanowić zabezpieczenie przed ujawnieniem danych uwierzytelniających zarówno poprzez zmniejszenie negatywnego wpływu ujawnienia, jak i poprzez pomoc w identyfikacji zmian w uprawnieniach użytkownika. Większa kontrola dostępu użytkowników oznacza, że wewnętrzne i zewnętrzne naruszenia bezpieczeństwa systemów mają mniejszy negatywny wpływ.

Zdarzenia, które występują w systemach IAM, powinny być również audytowane i monitorowane.

## PAM — zarządzanie dostępem uprzywilejowanym

**PAM** (ang. *Privileged Access Management*) to nazwa, którą określa się kontrolę nad uprzywilejowanym dostępem do kont, aplikacji i systemów w środowisku organizacji. W systemie komputerowym konto uprzywilejowane ma uprawnienia do omijania mechanizmów bezpieczeństwa oraz do zasadniczej zmiany programów i konfiguracji systemu. Przeciwnik zawsze będzie próbował podnosić swój poziom przywilejów w systemie, aby zdobyć i utrzymać nad nim kontrolę.

Posiadanie niektórych użytkowników z uprzywilejowanym dostępem jest zawsze potrzebne, ale sposób, w jaki te przywileje są przyznawane i zarządzane, może zminimalizować ryzyko nadużyć. Większość kont w organizacji powinna należeć do kategorii użytkowników standardowych/gości. Konta te mają ograniczony dostęp do zasobów, przy czym konta gości mają mniejsze uprawnienia w systemie. Uprawnienia użytkownika standardowego są zazwyczaj definiowane na podstawie roli, jaką pracownik pełni w firmie, oraz zadań, jakie ma wykonywać.

Każde konto, które ma możliwość udzielania dalszego dostępu innym kontom, jest kontem uprzywilejowanym. Na szczycie tej piramidy znajduje się superużytkownik (administrator lub *root*). Konto to powinno być używane przez wyspecjalizowanych pracowników IT, ponieważ ten typ użytkownika będzie miał nieograniczoną władzę nad systemem.

PAM i IAM pomagają zapewnić widoczność i monitoring użytkowników oraz dostępów. Prawidłowe monitorowanie uprzywilejowanych użytkowników i procesów może pomóc nam w wykryciu złośliwej hakerskiej aktywności w systemie. Ponadto ten rodzaj monitorowania jest obowiązkowy dla organizacji, które muszą być między innymi dostosowane do krajowych regulacji, takich jak SOX lub HIPAA.

## Systemy wykrywania włamań i zapobiegania im

**Systemy wykrywania włamań** (ang. *Intrusion Detection Systems*, IDS) lub **systemy zapobiegania włamaniom** (ang. *Intrusion Prevention Systems*, IPS) to systemy, które próbują wykryć, kiedy przeciwnik analizuje nasz system, aby ustalić, jak lepiej przeprowadzić atak. Systemy IDS i IPS analizują całe pakiety w poszukiwaniu podejrzanych zdarzeń. Jeśli takie zdarzenie zostanie znalezione, IDS rejestruje je i wysyła alert, natomiast IPS (zwany również *aktywnym* IDS) blokuje połączenie. Ze względu na podobieństwo do zapór tego typu systemy bezpieczeństwa są zintegrowane w ramach tzw. **zapór nowej generacji**, choć zakres ich możliwości zmienia się w zależności od producentów, którzy je stosują.

Istnieje wielu producentów oferujących rozwiązania zabezpieczające IDS/IPS, a dzienniki zdarzeń będą różne dla każdego z nich. Jednym z bardzo popularnych, wieloplatformowych rozwiązań IDS typu open source jest SNORT, który można pobrać za darmo z *https://www.snort.org/*.

Poniżej przedstawiono przykład loga SNORT zawierającego błędnie sformułowane pakiety IGAP i TCP wysłane przez atakującego:

```
[**] [1:2463:7] EXPLOIT IGMP IGAP message overflow attempt [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
02/18-14:03:05.352512 159.21.241.153 -> 211.82.129.66
IGMP TTL:255 TOS:0x0 ID:9744 IpLen:20 DgmLen:502 MF
Frag Offset: 0x1FFF Frag Size: 0x01E2
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2004-0367][
```

Kolejne dwa bardzo popularne IDS-y to Suricata i Bro/Zeek. Oba zapewniają dodatkową funkcjonalność na swój własny sposób. Suricata (*https://suricata-ids.org/*) jest wielowątkowa i może przechwytywać próbki złośliwego oprogramowania, zapisywać w dziennikach certyfikaty, żądania HTTP i DNS itd. Bro/Zeek (*https://www.zeek.org/*) przekształca przechwycony ruch w zdarzenia, które mogą być badane za pomocą języka skryptowego sterowanego zdarzeniami (skrypty Bro).

## ESS — pakiety bezpieczeństwa punktów końcowych

Kiedy z siecią firmową łączy się zdalne lub mobilne urządzenie, połączenie takie tworzy potencjalny punkt dostępu dla ewentualnych zagrożeń naruszających bezpieczeństwo. Jednak urządzenia mobilne będące własnością firmy również wymagają ochrony. **Pakiety bezpieczeństwa punktów końcowych** (ang. *Endpoint Security Suites*) starają się zminimalizować ryzyko zarówno dla urządzeń mobilnych, jak i dla samej organizacji. Pakiety bezpieczeństwa punktów końcowych składają się z centralnie zarządzanego oprogramowania zabezpieczającego, które weryfikuje poprawność działania urządzeń i w razie potrzeby aktualizuje ich oprogramowanie. Kontrola poprawności działania urządzenia może obejmować między innymi sprawdzenie poprawności zainstalowanych wersji określonego oprogramowania lub sprawdzenie konfiguracji zabezpieczeń określonego systemu operacyjnego. Produkt ten przynosi użytkownikowi wiele korzyści, ponieważ jest rozbudowany, a jego pełne możliwości różnią się w zależności od producenta. Można go zintegrować z ochroną antywirusową, zaporami i systemami wykrywania włamań (IDS).

Zazwyczaj pomiędzy pakietem bezpieczeństwa punktów końcowych a urządzeniami mobilnymi tworzona jest struktura serwer-klient. Urządzenia mają zainstalowanego agenta bezpieczeństwa, który regularnie komunikuje się z serwerem, pozwalając punktowi końcowemu na monitorowanie urządzenia.

## Zarządzanie oprogramowaniem antywirusowym

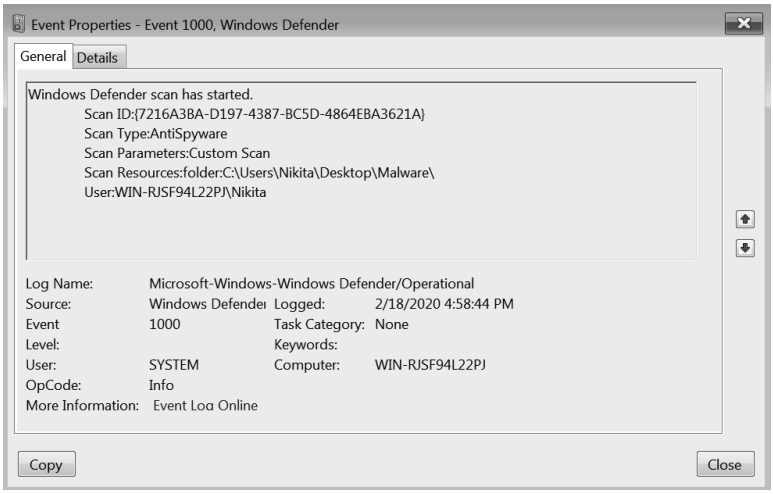
Prawdopodobnie najbardziej znanym mechanizmem bezpieczeństwa wśród przeciętnych użytkowników jest mechanizm **antywirusowy**. Antywirus (lub antimalware) to oprogramowanie, które służy do zapobiegania instalacji złośliwych plików. Jest on również używany do wykrywania innych złośliwych programów, które mogą być już w systemie, i usuwania ich.

Dzienniki tworzone przez oprogramowanie antywirusowe mogą być naprawdę przydatne. Należy pamiętać, że niektóre podmioty stwarzające zagrożenie używają bardzo specyficznych rodzin złośliwego oprogramowania. Jeśli więc widzimy, że nasz program antywirusowy wykrył wirusa, który dzięki naszym działaniom w zakresie wykrywania zagrożeń możemy powiązać z grupą generującą zaawansowane trwałe zagrożenia, możemy zbadać taktyki, techniki i procedury podmiotów stwarzających zagrożenie, aby znaleźć inne ślady ich aktywności w naszym środowisku.

Istnieje wiele dobrze znanych rozwiązań antywirusowych. Ich formaty dzienników będą się różnić w zależności od producenta. Poniżej znajduje się przykład dziennika pochodzącego z darmowego rozwiązania antywirusowego znanego jako AVG:

```
2/18/2020 6:14:44 PM C:\Users\Nikita\Desktop\Malware\
↪e3797c58aa262f4f8ac4b4ef160cded0737c51cb.exe [L] VBA:Downloader-BUB [Trj] (0)
File was successfully moved to Quarantine...
2/18/2020 6:17:49 PM C:\Users\Nikita\Desktop\Malware\
↪e3797c58aa262f4f8ac4b4ef160cded0737c51cb.exe [L] VBA:Downloader-BUB [Trj] (0)
File was successfully moved to Quarantine...
```

Rysunek 3.31 pokazuje logi programu Windows Defender w tym zakresie.




**Rysunek 3.31.** Widok dziennika zdarzeń programu Windows Defender

Od czasu systemu Windows Vista każdy system operacyjny Windows ma domyślnie zainstalowany program Windows Defender. Windows Defender jest komponentem antywirusowym systemu Windows, który jest natywnie zainstalowany w systemie. Dzienniki programu Windows Defender mogą być dostępne poprzez przeglądarkę dziennika zdarzeń systemu Windows, jak pokazano to na poprzednim zrzucie ekranu.

# Podsumowanie

W tym rozdziale omówiliśmy kilka podstawowych pojęć, które łowca zagrożeń musi zrozumieć, aby skutecznie przeprowadzać polowania i interpretować dostępne informacje. Omówiliśmy niektóre z najbardziej znanych narzędzi dostępnych w systemie Windows, jak również sposób, w jaki system Windows zapisuje zdarzenia w plikach dziennika. Wreszcie, przyjrzeliśmy się kompleksowej (ale nie kompletnej) liście możliwych źródeł danych potrzebnych do prowadzenia polowań na zagrożenia.

W następnym rozdziale dowiemy się, w jaki sposób mapować raporty wywiadowcze przy użyciu ATT&CK jako części procesu informatyki wywiadowczej. W kolejnych rozdziałach opowiemy sobie o tym, jak wykorzystać te mapowania do prowadzenia naszych polowań.

## To proste. Szukaj. Wykryj. Zneutralizuj!

Udany atak na system informatyczny organizacji może mieć bardzo poważne konsekwencje. W ostatnich latach analitycy cyberbezpieczeństwa starają się uprzedzać zagrożenia i je neutralizować, zanim dojdzie do wystąpienia większych szkód w systemie. Podejście to wymaga nieustannego testowania i wzmacniania mechanizmów obronnych w systemie informatycznym organizacji. W ramach tych procesów można zebrać wiele cennych danych, użyć ich do budowy modeli i dzięki temu lepiej zrozumieć istotne kwestie związane z bezpieczeństwem IT.

Ta książka to praktyczny przewodnik po aktywnych technikach wykrywania, analizowania i neutralizowania zagrożeń cybernetycznych. Dzięki niej, nawet jeśli nie posiadasz specjalistycznej wiedzy w tym zakresie, łatwo wdrożysz od podstaw skuteczny program aktywnego zabezpieczania swojej organizacji. Dowiesz się, w jaki sposób wykrywać ataki, jak zbierać dane i za pomocą modeli pozyskiwać z nich cenne informacje. Przekonasz się, że niezbędne środowisko możesz skonfigurować przy użyciu narzędzi open source. Dzięki licznym ćwiczeniom nauczysz się w praktyce korzystać z biblioteki testów Atomic Red Team, a także z frameworku MITRE ATT&CK™. Ponadto zdobędziesz umiejętności związane z dokumentowaniem swoich działań, definiowaniem wskaźników bezpieczeństwa systemu, jak również komunikowaniem informacji o jego naruszeniach swoim współpracownikom, przełożonym i partnerom biznesowym.

**Dzięki książce:**

- poznasz podstawy informatyki śledczej i analizy zagrożeń
- dowiesz się, w jaki sposób modelować zebrane dane i dokumentować wyniki badań
- nauczysz się symulować działania agresorów w środowisku laboratoryjnym
- wprawisz się we wczesnym wykrywaniu naruszeń
- poznasz zasady komunikowania się z kierownictwem i otoczeniem biznesowym

**Valentina Costa-Gazcón** — argentyńska analityczka cyberbezpieczeństwa, specjalizuje się w śledzeniu zaawansowanych trwałych zagrożeń. Jest samoukiem w dziedzinie programowania i analizy zagrożeń. Jest również jednym z najważniejszych członków grupy Open Threat Research.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
*Sięgnij po więcej!*

ISBN 978-83-283-8885-7

Cena: 89,00 zł

Packt>