Bezpieczeństwo systemów operacyjnych

Systemy wykrywania i zapobiegania włamaniom

Arkadiusz Chrobot

Katedra Systemów Informatycznych

6 listopada 2026

Plan

1. Wstęp
2. Klasyfikacja IDPSs
3. Metody detekcji
4. Architektura
5. Konfiguracja
6. Typy IDPS
7. Przykłady
8. Literatura

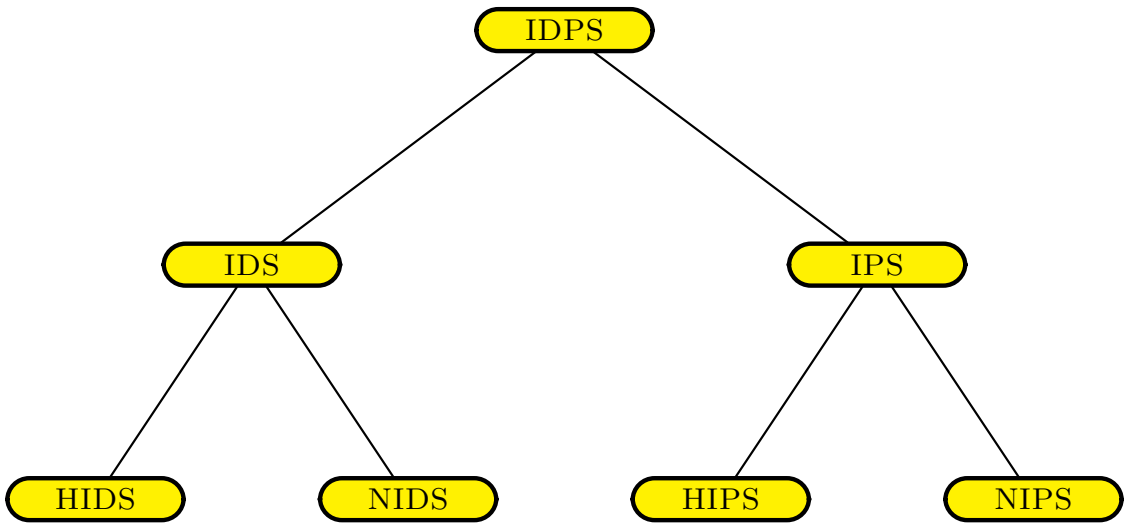
Wstęp

Koncepcja automatycznego wykrywania naruszenia zabezpieczeń w systemach komputerowych powstała w latach 80. ubiegłego stulecia. Za jeden z najbardziej znaczących momentów w początkach jej istnienia uważa się opublikowanie przez Dorothy E. Denning artykułu poświęconego modelowi wykrywania włamań [1]. Autorka argumentuje w nim, że budowa całkowicie bezpiecznych systemów komputerowych nie tylko jest trudna lub wręcz niemożliwa, bo może uniemożliwiać tym systemom udostępnianie wymaganych usług. Bardziej ekonomicznym i użytecznym rozwiązaniem jest zbudowanie systemu mniej zabezpieczonego, ale wykrywającego niedozwolone działania. Głównym zagadnieniem poruszanym w artykule jest model wykrywania włamań, bazujący na założeniu, że naruszenie bezpieczeństwa wiąże się z odbiegającymi od normy operacjami wykonywanymi w systemie. Aby było to możliwe oprogramowanie odpowiedzialne za ten rodzaj monitoringu musi korzystać z odpowiednich usług i zasobów udostępnianych przez system operacyjny.

Wstęp

Za bezpośrednią implementację pomysłu opisanego na poprzednim slajdzie należy uznać systemy wykrywania włamań (ang. *Intrusion Detection System(s)* — IDS(s)) [3], które następnie dały początek systemom zapobiegania (lub przeciwdziałania) włamaniom (ang. *Intrusion Prevention System(s) — IPS(s)*) [4]. Ponieważ rozwiązania typu IPS dokonują także detekcji naruszania zabezpieczeń, to dosyć często określa się je mianem systemów wykrywania i zapobiegania włamaniom (ang. *Intrusion Detection and Prevention System(s) — IDPS(s)*), jednakże ta nazwa jest także stosowana do opisywania obu rozwiązań i w taki sposób będzie wykorzystywana w ramach wykładu [2]. Z IDS i IPS wywodzą się także SIEM (ang. *Security Information and Event Management*) — oprogramowanie gromadzące i analizujące informacje o zdarzeniach z różnych źródeł, EDR (ang. *Endpoint Detection and Response*) — programy chroniące urządzenia końcowe, XDR (ang. *Extended Detection and Response*) — narzędzia chroniące całe infrastruktury sieciowe.

Klasyfikacja IDPSs



Klasyfikacja systemów wykrywania i zapobiegania włamaniom (IDPSs)

Klasyfikacja IDPSs

Źródła dotyczące IDPSs różnie je klasyfikują, czasem w rozbieżny sposób. Objaśnienie skrótów występujących na poprzednim slajdzie jest następujące:

- **IPDS** system wykrywania i zapobiegania włamaniom,
- **IDS** system wykrywania włamań,
- **IPS** system zapobiegania włamaniom,
- **HIDS** system wykrywania włamań na poziomie urządzenia,
- **NIDS** system wykrywania włamań na poziomie sieci,
- **HIPS** system zapobiegania włamaniom na poziomie urządzenia,
- **NIPS** system zapobiegania włamaniom na poziomie sieci.

Klasyfikacja IDPSs

Głównym zadaniem IDS jest wykrywanie i powiadamianie o incydentach świadczących o trwającym lub wykonanym ataku. Działanie IPS również obejmuje te czynności, ale dodatkowo może on próbować przerwać trwający atak poprzez m.in. [4, 2]:

- blokowanie zagrażającego ruchu sieciowego, przez zmianę reguła zapory sieciowej lub przekierowanie go do systemu typu *honey-pot*;
- usunięcie szkodliwej zawartości w postaci np. ładunku w pakiecie lub załącznika do wiadomości e-mail;
- uruchomienie innych mechanizmów bezpieczeństwa, np. ustawień routera;
- wymuszenie polityki bezpieczeństwa, np. poprzez zablokowanie dostępu do określonego zasobu nieuprawnionemu użytkownikowi.

Metody detekcji

Detekcja naruszenia zasad bezpieczeństwa może być wykonywana przez IDPS przy użyciu pojedynczej metody, ale częściej spotykane są rozwiązania, które stosują kombinację kilku sposobów. Najczęściej używane techniki detekcji bazują na:

- sygnaturach (ang. *signature-based*),
- wykrywaniu anomalii (ang. *anomaly-based*),
- analizie stanu protokołu (ang. *stateful protocol analysis*)
- polityce bezpieczeństwa (ang. *policy-based*).

Istnieją również inne, rzadziej stosowane.

Metody detekcji

Detekcja bazująca na sygnaturach

Sygnatura jest wzorcem opisującym określony typ ataku. Wykrywanie naruszeń bezpieczeństwa polega na sprawdzeniu, czy obserwowane zachowanie jest zgodne z tym wzorcem. Przykładowo, duża liczba nieudanych prób uwierzytelnienia może świadczyć o trwającym ataku typu *brute force*. Ta metoda wykrywania jest efektywna przeciwko znanym atakom, pod warunkiem, że nie istnieje wiele ich wariantów. Niestety, nie można nią wykryć ataków, które do tej pory nie były znane. Jest ona także zawodna w przypadku niektórych technik omijania, polegających na ukryciu ataku. Metoda bazująca na sygnaturach jest prosta do zaimplementowania, ale nie pozwala korelować różnych zdarzeń, a więc nie wykrywa także ataków złożonych.

Metody detekcji

Wykrywanie anomalii

Wykrywanie anomalii bazuje na statystyce lub technikach uczenia maszynowego. Jego działanie sprowadza się do ustalenia profilu normalnego działania systemu i porównywania z nim bieżącego zachowania, celem znalezienia zdarzeń, które znacząco odbiegają od normy. Profil tworzony jest w procesie uczenia, które może zająć stosunkowo długi czas. Może on mieć charakter statyczny, czyli nie zmieniać się do chwili, gdy użytkownik IDPS wyda polecenie wygenerowania nowego lub dynamiczny, czyli podlegać ciągłej aktualizacji. W pierwszym przypadku każda istotna zmiana w systemie może generować fałszywie dodatnie wyniki. Drugi przypadek generuje ich znaczenie mniej, ale narażony jest na uznanie za normę potencjalnego ataku, który jest rozłożony w czasie. Tworzenie profilu zachowania jest szczególnie trudne dla urządzeń mobilnych, takich jak laptop, które często zmieniają środowisko sieciowe. Metoda detekcji anomalii jest efektywna w wykrywaniu ataków, które nie były znane uprzednio, ale może generować dużą liczbę fałszywie dodatnich wyników.

Metody detekcji

Analiza stanowa protokołu

Analiza stanowa protokołu jest rzadziej stosowaną metodą detekcji, w porównaniu z dwoma poprzednimi i raczej jest częściej spotykana w NIPS/NIDS niż HIPS/HIDS. Ma ona cechy zarówno metod bazujących na sygnaturach, jak i wykrywających anomalie. W niej również używane są profile opisujące poprawne zachowanie określonych protokołów sieciowych, ale są one dostarczane przez twórcę IDPS, a nie powstają w wyniku uczenia. Podstawą do tworzenia tych profili są najczęściej dokumenty RFC lub standardy IEEE.
Tą metodą można badać protokoły warstwy sieciowej, transportowej i aplikacji, które posiadają stan. Przykładowo, nadaje się ona dla TCP, ale nie dla UDP. Oprócz stanu protokołu w tej metodzie wykonywane są dodatkowe weryfikacje, jak np. liczba i długość parametrów. Metoda ta jest zasobochłonna i nie wykrywa ataków, które nie naruszają profili protokołów. Dodatkową trudność w jej stosowaniu powodują niestandardowe implementacje protokołów.

Metody detekcji

Metoda bazująca na polityce bezpieczeństwa

Ta metoda, zgodnie z nazwą wykrywa w monitorowanym systemie naruszenia polityki opracowanej przez zespół do spraw bezpieczeństwa [4]. Przykładowo, polityka może zawierać reguły określające, którzy użytkownicy i w jakich okolicznościach mogą korzystać z określonych zasobów. Jeśli IDPS stosujący metodę wykrywania włamań opierającą się na tej polityce zauważy, że dany użytkownik próbuje uzyskać dostęp do systemu poza wyznaczonymi godzinami, to zablokuje tę próbę. Wykrywanie bazujące na polityce bezpieczeństwa oferuje duże możliwości dostosowania do potrzeb użytkowników, ale wymaga dużego nakładu pracy związanej z początkową konfiguracją, aby je poprawnie wdrożyć.

Metody detekcji

Inne metody

Jako przykład innych rozwiązań problemu wykrywania włamań można wskazać metodę bazującą na reputacji (ang. *reputation-based detection*) [3, 4]. Polega ona na sprawdzaniu źródła zdarzeń. Jeśli jest ono niezaufane, to zdarzenia zostaną zablokowane. Przykładem może być blokowanie przez IPS ruchu sieciowego pochodzącego z domeny lub adresu IP o złej reputacji.

Architektura

Typowe komponenty IDPS obejmują [2]:

czujniki lub agenty monitorują i analizują działania w systemie; czujniki związane są z sieciowymi IDPS, a agenty z instalowanymi na urządzeniach,

serwer zarządzający otrzymuje informacje od agentów lub czujników i nimi zarządza; niektóre z tych serwerów wykonują korelację zdarzeń; mogą nie występować wcale, lub pracować w większej liczbie,

bazę danych przechowuje dane nasyłane przez czujniki/agenty i serwer zarządzający; jest opcjonalna,

konsolę oprogramowanie, które służy do konfigurowania i/lub monitorowania IDPS.

Architektura

Komponenty IDPS mogą ze sobą współpracować poprzez zwykłą sieć (HIDS/HIPS) lub przy pomocy specjalnie wydzielonej sieci zarządzającej (NIDS/NIPS). To drugie rozwiązanie ma zaletę w postaci odizolowania ruchu sieciowego związanego z działaniem IDPS od pozostałego. Wymaga ono jednak wsparcia sprzętowego w postaci dodatkowego interfejsu sieciowego oraz odpowiedniej konfiguracji, która zapobiega przepływowi pakietów między interfejsami sieciowymi w tym samym urządzeniu. Serwery zarządzające, bazy danych oraz konsole powinny być podłączone wyłącznie do sieci zarządzającej. Dzięki temu IDPS staje się bardziej odporny na ataki i trudny do wykrycia dla adwersarzy. Sieć zarządzająca powinna być zrealizowana jako fizyczna, ale z uwagi na koszty lub brak odpowiednich komponentów sprzętowych może być zaimplementowana jako VLAN, choć wtedy nie będzie zapewniała całkowitego odizolowania ruchu sieciowego zarządzającego IDPS od produkcyjnego.

Konfiguracja

Konfiguracja IDPS może dotyczyć wielu aspektów jego działania i opierać się na takich rozwiązaniach jak:

progi (ang. *tresholds*) są wartościami, które rozgraniczają zachowanie poprawne od anormalnego;

czarne i biała listy definiują jakie zachowania są dozwolone, a jakie zabronione; czarne listy mogą np. zawierać numery portów, które nie powinny być używane, nazwy plików, które nie powinny być zmieniane; niektóre IDPS mogą je generować automatycznie; białe listy określają dozwolone zachowania, by zredukować liczbę wyników fałszywie dodatnich,

ustawienia alarmów (ang. *alert settings*) pozwalają włączyć lub wyłączyć określone typy alarmów lub określić kiedy je ignorować;

edycja i przegląd kodu pozwala zmieniać sygnatury lub profile protokołu, lub dowolne zachowanie systemu (w przypadku IDPS typu open source).

Typy IDPSs

Oprócz typów IDPSs wymienionych w klasyfikacji na początku wykładu należy także uwzględnić te, które są przeznaczone dla sieci bezprzewodowych (ang. *wireless*) oraz związane z analizą dużych wolumenów ruchu sieciowego (ang. *Network Behaviour Analysis* — NBA), historycznie znanych pod wieloma innymi nazwami, jak oprogramowanie do wykrywania anomalii zachowania ruchu sieciowego (ang. *Network Behaviour Anomaly Detection — (NBAD)*, oprogramowanie do analizy anomalii zachowania ruchu sieciowego i reakcji (ang. *network behaviour analysis and response software*) oraz oprogramowanie do wykrywania anomalii sieciowych (ang. *network anomaly detection software*). Każde z tych rozwiązań ma określone zalety i zastosowania, ale również posiada pewne ograniczenia. Dlatego często w systemach komputerowych stosowane jest więcej niż jedno. Jeśli pochodzą one od jednego producenta, to możliwość ich integracji może być przewidziana w projekcie. W innych przypadkach komunikacja między nimi może odbywać się przy pomocy znanych protokołów, np. *syslog*.

Typy IDPSs

NIDS/NIPS

Czujniki (ang. *sensors*) w przypadku rozwiązań NIPS/NIDS są instalowane na perymetrach sieci lub jej segmentów, celem monitorowania ruchu pakietów. Zazwyczaj są one umiejscowione za zaporą sieciową, aby wykrywać ataki, które są przez nią pomijane. Nowoczesne zapory zawierają dosyć często takie systemu jako jeden ze swoich komponentów. NIDS/NIPS mogą analizować protokoły warstwy aplikacji, transportowej i sieci. Rzadziej zdarza się, że wykonują ograniczoną analizę protokołów z warstwy fizycznej np. ARP.
Czujniki NIPS występują w dwóch wersjach: liniowej (ang. *inili-ne*) i pasywnej (ang. *passive*). Pierwsze badają rzeczywisty ruch i bezpośrednio mogą blokować ataki. Drugie analizują kopie ruchu sieciowego. W ich przypadku próby zapobiegania atakom sprowadzają się do wysłania pakietów, które kończą połączenie. Czujnikom nie są przypisywane adresy IP, aby je ukryć (ang. *stealth*). Korzystają one z trybu bezładnego (ang. *promiscuous*) pracy interfejsu sieciowego.

Typy IDPSs

NIDS/NIPS

NIDS/NIPS oferują duże możliwości w zakresie wykrywania zagrożeń, stosując kombinację metod bazujących na sygnaturach, detekcji anomalii i analizie stanu protokołu. Pozwala im to wykrywać działania związane nie tylko z właściwym atakiem, ale również z przygotowującym do niego rekonesansem. Dodatkowo mogą one odnajdować próby tunelowania ruchu, tylne furtki, urządzenia wykonujące nieautoryzowane usługi oraz naruszenia polityki bezpieczeństwa (np. używanie nieuprawnionych portów). Niektóre z nich uwzględniają topologię sieci, co pozwala im nadać odpowiednie priorytety wykrywanym zdarzeniom. Czujniki wymagają jednak odpowiedniego dostrojenia (ang. *tunning*) do charakterystyki monitorowanego ruchu sieciowego.

Typy IDPSs

NIDS/NIPS

W zakresie działań prewencyjnych, podstawowym działaniem pasywnych sensorów jest próba zatrzymania ataku przez wysłanie do obu stron pakietów kończących połączenie, co działa jedynie w przypadku protokołów posiadających taką możliwość (np. TCP) i nie daje szybkiego skutku. W tym zakresie więcej możliwości oferują czujniki liniowe, które mogą blokować i modyfikować złośliwe pakiety oraz zmniejszać przepustowość łącza. Oba rodzaje czujników mogą także uruchamiać inne mechanizmy zabezpieczające.

Typy IDPSs

NIDS/NIPS

Czujniki NIDS/NIPS nie mogą wykryć ataków dokonywanych zaszyfrowanymi połączeniami (np. VPN, SSH, HTTPS). Dlatego powinny być one instalowane w miejscach, gdzie mogą odczytać ładunek zanim zostanie on zaszyfrowany lub tuż po jego zdeszyfrowaniu. W przypadku dużego ruchu sieciowego czujniki mogą nie przeprowadzać pełnej analizy. Są także wrażliwe na zagubienia pojedynczych pakietów. W rozwiązaniu tych problemów może pomóc odpowiednie wsparcie sprzętowe lub zmiana ustawień. Czujniki są także wrażliwe na kilka rodzajów ataków. Jednym z najprostszych są ataki DoS/DDoS, ale istnieją również takie, które polegają na „oślepianiu" czujnika poprzez wysłanie do niego dużej liczby „podejrzanych" pakietów. Pozwala to adwersarzowi wykonać atak innymi kanałami.

Typy IDPSs

Bezprzewodowe IDPS

Bezprzewodowe IDPS to systemy wykrywania i zapobiegania włamaniom, które zostały przygotowane na potrzeby sieci bezprzewodowych. Ponieważ tego typu sieci korzystają z dwóch typów pasma (2,4 GHz oraz 5 GHz), które podzielone są na osobne kanały, to IDPS przeznaczony dla nich nie może badać wszystkich pakietów równocześnie, chyba że ma odpowiednie wsparcie sprzętowe w postaci osobnych modułów radiowych. Częściej spotykanym rozwiązaniem jest jednak próbkowanie ruchu bezprzewodowego nazywane skanowaniem kanałów. W związku z tym IDPSs dla sieci WLAN działają jedynie w zakresie protokołów związanych z obsługą sieci bezprzewodowych. Czujniki dla tego typu IDPS mogą być instalowane na urządzeniach mobilnych, przełącznikach lub punktach dostępowych.

Typy IDPSs

Bezprzewodowe IDPS

IDPS przeznaczone dla sieci bezprzewodowych mogą wykrywać nielegalne lub słabo zabezpieczone urządzenia sieciowe, a także nieautoryzowane sieci WLAN. Większość czujników tych IDPS pozwala ustalić fizyczne położenie danego urządzenia przy pomocy triangulacji. Zazwyczaj IDPS przeznaczone dla sieci bezprzewodowych generują zdecydowanie mniej fałszywie dodatnich wyników niż pozostałe systemy tego typu, ale także mogą wymagać dostrojenia do konkretnego środowiska. W zakresie prewencji czujniki mogą nakazywać urządzeniu lub urządzeniom rozłączenie i odmawiać ponownego przyłączenia. Mogą także rekonfigurować punkty dostępowe lub przełączniki, aby nie przyjmowały połączeń od urządzeń o określonych adresach MAC.

Typy IDPSs

Bezprzewodowe IDPS

IDPSs przeznaczone dla sieci bezprzewodowych mogą nie wykrywać krótkich ataków, z uwagi na konieczność skanowania kanałów. Nie są one także przeznaczone do wykrywania ataków pasywnych, w których adwersarz zapisuje przechwycony ruch, aby go potem przeanalizować. Czujniki dla takich systemów mogą także okazać się nieodporne zarówno na ataki logiczne typu DoS, jak i fizyczne.

Typy IDPSs

NBA

IDPS należące do klasy NBA badają duże wolumeny ruchu sieciowego celem wykrycia ataków typu DDoS, określonych typów złośliwego oprogramowania (np. robaki, tylne furtki) oraz naruszeń polityki bezpieczeństwa. NBA może stosować te same rodzaje czujników co NIDS/NIPS, ale posiada również specjalizowane, które otrzymują informację o przepływie pakietów od routerów lub innych urządzeń sieciowych. Większość NBA nie stosuje metod detekcji bazujących na sygnaturach, a ich działanie opiera się głównie na wykrywaniu anomalii i w mniejszym stopniu na analizie stanu protokołów. Z uwagi na badanie przez nie dużych ilości danych mogą one nie tylko wykryć, ale pozwolić odtworzyć ścieżkę niektórych z wymienionych wcześniej ataków. Z tego również powodu moment wykrycia ataku może być odległy od chwili jego rozpoczęcia. Czujniki NBA oferują duże możliwości prewencji obejmujące wysyłanie pakietów kończących połączenia, blokowanie połączeń, a nawet rekonfigurację innych mechanizmów bezpieczeństwa.

Typy IDPSs

NBA

Niestety, NBA mają także poważne ograniczenia, z których najpoważniejszym jest późna detekcja ataków, co może być istotne w przypadku zagrożeń typu DDoS lub infekcji złośliwym oprogramowaniem. Opóźnienie to wynika nie tylko z prowadzonej przez NBA analizy, ale także z faktu, że systemy te otrzymują dane w postaci wsadów, które są im dostarczane w stosunkowo długich odstępach czasu (nawet do 1 godziny). Alternatywne rozwiązanie, polegające na analizie ruchu przez same czujniki NBA może być zbyt zasobochłonne.

Typy IDPSs

HIDS/HIPS

Działanie HIDS/HIPS ogranicza się do zdarzeń pojawiających się na pojedynczym urządzeniu, zazwyczaj końcowym, choć są także systemy tego typu instalowane na urządzeniach sieciowych. Agenty tych systemów monitorują dzienniki systemowe, uruchomione procesy, operacje na plikach (dostęp i modyfikację), zmiany konfiguracji aplikacji i systemu, a także wychodzący i przychodzący ruch sieciowy. Niektóre systemy HIDS/HIPS są przeznaczone do monitorowania określonego oprogramowania, dlatego nazywane są *application-based* IDPS.

Typy IDPSs

HIDS/HIPS

Agenty HIDS/HIPS są instalowane zazwyczaj na systemach o krytycznym znaczeniu. Stosują one wszystkie opisane wcześniej metody detekcji, a nad czujnikami NIDS/NIPS mają tę przewagę, że posiadają dostęp do niezaszyfrowanych danych. W zakresie prewencji zmieniają one architekturę oprogramowania na chronionym urządzeniu, wprowadzając warstwy pośredniczące, nazywane podkładkami (ang. *shims*), między istniejące komponenty oprogramowania (np. wywołania systemowe), aby móc monitorować i blokować niepożądane działania. HIDS/HIPS oferują możliwości w zakresie analizy kodu, badania i filtrowania ruchu sieciowego, monitorowania systemu plików i analizy dzienników zdarzeń. Potrafią także określać, czy atak zakończyłby się powodzeniem, gdyby nie został zatrzymany. Z uwagi na mniejszą informację o kontekście działań dostępną dla HIDS/HIPS, systemy te mogą być mniej dokładne niż pozostałe omawiane. Tę dokładność można zwiększyć używając odpowiedniej kombinacji metod detekcji.

Typy IDPSs

HIDS/HIPS

HIDS/HIPS mogą także wymagać bardziej rozległego i dokładnego strojenia niż inne systemy z tej kategorii. Szczególnie dotyczy to parametrów HIDS/HIPS instalowanych na urządzeniach przenośnych. HIPS mogą powstrzymywać ataki poprzez neutralizację złośliwego oprogramowania, blokowanie złośliwego ruchu sieciowego zanim zostanie on przetworzony, niedopuszczanie do umieszczenia na urządzeniach plików z niebezpieczną zawartością i przeprowadzania nieautoryzowanych operacji na plikach konfiguracyjnych.
Niektóre metody wykrywania, np. bazujące na analizie logów, nie pozwalają zatrzymywać ataków, bo identyfikują zdarzenia po ich zajściu. Ponadto, niektóre agenty są zaprojektowane, aby przekazywać dane do innych systemów bezpieczeństwa w określonych, zazwyczaj długich, przedziałach czasu, co może opóźniać detekcję ataków. Niemniej większość z nich działa w czasie rzeczywistym. Wadami HIDS/HIPS są także duże zapotrzebowanie na zasoby oraz potencjalne konflikty działania z innymi mechanizmami bezpieczeństwa.

Przykłady IDPSs

Wśród IDPSs należących do kategorii open source można wymienić Suricata, Snort, Wazuh, Security Onion, tripwire, fali2ban. Natomiast do komercyjnych zaliczane są rozwiązania oferowane przez Palo Alto Networks (Palo Alto Networks Firewall/IPS), Cisco (Cisco Secure Firewall/IPS), Fortinet (Fortinet FortiGate), TrendMicro (TrippingPoint).

Literatura



D.E. Denning. An Intrusion-Detection Model. *IEEE Transactions on Software Engineering*, SE-13(2):222–232, 1987. DOI: 10.1109/TSE.1987.232894.



Karen Scarfone i Peter Mell. Intrusion Detection and Prevention Systems. 2013. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901146.



What is an intrusion detection system (IDS)? URL: https://www.ibm.com/think/topics/intrusion-detection-system (termin wizyty 02. 11. 2026).



What is an intrusion prevention system (IPS)? URL: https://www.ibm.com/think/topics/intrusion-prevention-system (termin wizyty 02. 11. 2026).

Pytania

?

KONIEC

Dziękuję Państwu za uwagę!