Włamania do cyberprzestrzeni

Cyberbezpieczeństwo to środki wbudowane w informacje system podczas procesu rozwoju.

Wprowadzenie

Włamanie, w kontekście systemów informatycznych, stanowi naruszenie ustalonych zasad dostępu do danych, przy czym naruszenie może dotyczyć odczytu lub modyfikacji chronionych danych. Systemy informacyjne są chronione przez dedykowane systemy analizy ruchu zaprojektowane do wykrywania i, miejmy nadzieję, blokowania włamań. Takie systemy wykonane ze sprzętu i / lub oprogramowanie, są określane jako systemy wykrywania i zapobiegania włamaniom. W zależności od konkretnej aplikacji, system może być systemem IDS, to znaczy tylko systemem wykrywania włamań bez możliwości zapobiegania, lub może być systemem IDPS, czasem wciąż określanym jako IDS, który ma zarówno funkcje, wykrywanie, jak i zapobieganie. IDPS wdrażają reguły ustanowione przez administratora bezpieczeństwa, mające zastosowanie do ochrony punktów dostępu lub wejścia. W oparciu o te zasady IDPS przekazuje, blokuje, opóźnia lub przekierowuje ruch danych. Wybrane działanie nie może odbywać się z ludzką prędkością, a zatem wymaga od eksperta systemu, najlepiej ze sztuczną inteligencją, do decydowania z elektroniczną prędkością o potrzebnym działaniu. IDPS są ogólnie podzielone na cztery rodzaje systemów, a mianowicie

• W oparciu o sieć

• Host-Based

• Analiza zachowania sieci

• Bezprzewodowy

Wymagania IDPS to mapa polityki bezpieczeństwa organizacji w kierunku włamań.

USŁUGI BEZPIECZEŃSTWA	**:**	**UWAGI OPERACYJNE**
Monitorowanie	:	Skalowalności
Urządzenia	:	Niezawodność
Funkcje	:	Interoperacyjność
Możliwości	:	Rekonfiguracja
Wykrywanie	:	Dokumentacja
Zapobieganie	:	Wsparcie techniczne
Raportowanie	:	Szkolenie
WYDAJNOŚĆ	**:**	**SKUTECZNOŚĆ**
Obliczeniowy	:	Koszt początkowy
Przechownie	:	Koszt konserwacji

Wdrożenie tych wymagań opiera się na dostępnych technologiach zastosowanych do przewidywanych potrzeb, z parametrem opłacalności. Istnieje szeroka gama narzędzi IDPS, które zapewniają monitorowanie zdarzeń i bezpieczeństwo systemu informatycznego w stosunku do znanych zagrożeń. Najważniejszym celem intruza jest mechanizm ochronny systemu informatycznego. Początkowo, poprzez różnorodne ataki, intruzi próbują określić mocne i słabe strony IDPS, próbując rozpoznać

obecność luk w zabezpieczeniach, przez które mogą wejść do systemu i uzyskać dostęp do uszkodzonych zasobów lub uszkodzić je. Takimi zasobami mogą być listy haseł, pliki wrażliwych treści lub mechanizmy dostępu.

Konfiguracja IDPS

Ogólnie rzecz biorąc, każdy system składa się z trzech głównych komponentów: czujników, w których dane są gromadzone ze środowiska i częściowo przetwarzane; procesor, który podejmuje decyzje w wyniku oceny danych i korelacji; oraz siłowniki, które napędzane przez procesor wpływają na środowisko. Podobnie w przypadku IDPS istnieją czujniki, oprogramowanie przetwarzające oraz dotknięte nimi jednostki lub funkcje.

Czujniki

Czujniki są istotnymi elementami procesu wykrywania włamań, których funkcją jest rozpoznawanie wystąpienia potencjalnie szkodliwych zdarzeń. Lokalizacja czujników w systemie informacyjnym jest niezwykle ważna i ma ogromne znaczenie. Dlatego przed zidentyfikowaniem lokalizacji czujników należy dokładnie ustalić topologię systemu informacyjnego. Takie lokalizacje są punktami wejścia do funkcji lub obszarów systemu. Typowymi przykładami są interfejsy korporacyjne do świata zewnętrznego, takie jak połączenia z Internetem za pośrednictwem sieci LAN lub WLAN, a także zdalny dostęp za pośrednictwem modemów. W przypadku organizacji podzielonych na działy czujniki mogą być również umieszczane w międzywydziałowych punktach wejścia, monitorując dostęp do cennych zasobów w ramach działu. Bardzo ważne są również interfejsy ekstranetowe. Są to punkty wejścia, w których partnerzy będą uzyskiwać dostęp i ewentualnie modyfikować, jeśli zostaną autoryzowane, krytyczne dane w korporacyjnych bazach danych. Zdarzały się przypadki, gdy intruz z sieci A wchodzi do sieci korporacyjnej B za pośrednictwem ekstranetu A – B, a podczas gdy w B, poprzez ekstranet B – C, uzyskuje dostęp do sieci korporacyjnej C, na którą intruz nie miał autoryzacji. To wyraźnie pokazuje, że organizacja B ponosi odpowiedzialność w stosunku do swoich partnerów ekstranetowych.

Nie można nie doceniać podatności sieci wewnątrz korporacyjnej, a czujniki należy umieszczać na przejściach międzywydziałowych. Tak więc topologia sieci korporacyjnej i lokalizacja krytycznych zasobów są dobrze znane przed umieszczeniem czujników. Równie ważne jest, aby czujniki były odpowiednio zaprogramowane pod kątem tego, czego będą „szukać". Umieszczone w strategicznych lokalizacjach czujniki monitorują ruch zgodnie z określonymi kryteriami. Oznacza to, że czujniki szukają wystąpienia określonych zdarzeń i zgłaszają się do agentów. Agenci to oprogramowanie, które odbiera obserwacje czujników i ocenia, jakie zagrożenie może stwarzać samo zdarzenie lub w połączeniu z innymi zdarzeniami. Agenci mają sztuczną inteligencję, co oznacza, że podejmują decyzje na podstawie kryteriów, które mogą ulec zmianie w zależności od różnych okoliczności. Ponadto dzięki bezpiecznej komunikacji między agentami agenci wspólnie monitorują całą sieć przedsiębiorstwa. Dane z czujników mogą być tak proste, jak zliczanie liczby awarii próby podania nazwy użytkownika lub hasła. Na podstawie tej liczby agent decyduje o wymaganej akcji. Parametrem, który może statystycznie dostarczyć informacje, jest odstęp czasu między przesłaniem nazwy użytkownika a hasłem. Ten interwał wskazuje czas, jaki zajęło użytkownikowi wprowadzenie hasła. Strona hasła może mieć krótki kod wykonywalny, który zlicza odstępy czasu między wpisanymi znakami. Dotyczy to wpisu nazwy użytkownika lub hasła. Wytworzona dynamika naciśnięć klawiszy może statystycznie zapewnić dość wiarygodny mechanizm uwierzytelniania semibiometrycznego, służący jako cyfrowa identyfikacja użytkownika. Czujniki mogą być umieszczone w linii z przepływem danych służących jako zapora ogniowa. Będąc w linii czujnik może blokować podejrzany ruch, zapobiegając w ten sposób realizacji próby ataku. Czujniki mogą znajdować się z boku, dotykając przepływu ruchu i wysyłając zebrane dane do procesora IDPS. Będąc z boku, czujnik biernie obserwuje ruch bez wpływu na prędkość sieci.

Oczywiście nie może blokować podejrzanego ruchu. Tak czy inaczej, wyniki czujników są przekazywane do procesora IDPS, skąd może dojść do działania blokującego.

Procesor

Procesor zbiera zarejestrowane działania dostarczone przez czujniki i agentów i koreluje je w poszukiwaniu identyfikacji złośliwego oprogramowania lub nieprawidłowych sytuacji. Wydajność musi być dokładnie przetestowana - z IDPS offline i online - z ciągle aktualizowanymi kryteriami, aby odzwierciedlić najnowsze technologie obronne, a także stale rozwijające się możliwości szkodliwego oprogramowania.

Konsole

Procesor dostarcza wszystkie ustalenia do konsol, gdzie administratorzy nadzorują wydajność systemu. Parametry wykrywania i przetwarzania mogą być regulowane przez procesor w czasie rzeczywistym lub przez działania administratora.

Sieć

Komponenty IDPS - czujniki, procesor i konsole - komunikują się ze sobą za pomocą własnej sieci, niezależnej od sieci produkcyjnej, która jest dostępna przez Internet. W ten sposób IDPS staje się odporny na ataki włamaniowe, ponieważ jest fizycznie lub logicznie izolowany od sieci.

Możliwości IDPS

Możliwości IDPS różnią się w zależności od stopnia zaawansowania systemu. Jednak w minimalnym stopniu dyrektor ds. Informacji (CIO) użyje IDPS do niezależnego potwierdzenia działania zapory, oceny oczekiwanej zdolności filtrowania i ostrzegania, a także do powiadomienia o nietransakcyjnych czynnościach, takich jak skanowanie IP lub skanowanie portów, które, choć nie zagrożenie jest prekursorem możliwego zbliżającego się ataku włamaniowego. W procesie nadzoru nad przypisaną działalnością IDPS rejestrują informacje związane z nimi i zgłaszają się do różnych organów, zgodnie z zaprogramowaniem. Takie wydania mogą być planowymi raportami wydawanymi w określonych punktach czasowych, raportami wyjątków wydawanymi automatycznie, ponieważ miało miejsce zdarzenie specjalne, lub raportami na żądanie, w których autoryzowani odbiorcy mogą otrzymywać raporty niestandardowe. Ponadto w przypadku rozpoznanego włamania IDPS może gromadzić i rozpowszechniać informacje peryferyjne, które mogą później pomóc w dochodzeniu kryminalistycznym dotyczącym włamania. Podstawowe możliwości IDPS można zaklasyfikować jako

• Pozyskiwanie informacji

• Rejestrowanie informacji

• Techniki wykrywania

• Działania zapobiegawcze

Pozyskiwanie informacji

Zbieranie informacji odbywa się za pomocą czujników, które zapewniają wstępne przetwarzanie przed przesłaniem wyników do procesora IDPS.

Rejestrowanie informacji

Rejestrowanie zdarzeń wraz z ich klasyfikacją powoduje gromadzenie dużej ilości danych związanych z wykrytymi zdarzeniami.

1. Znacznik czasu: data i godzina. Często IDPS może mieć własne zegary czasowe, aby najlepiej utrzymać dokładne zapisy.

2. Adresy: źródło i miejsce docelowe (IP, MAC, IMEI)

3. Numery portów: źródło i miejsce docelowe

4. Typy portów: typy i kody TCP, UDP lub ICMP

5. Protokół warstwy: sieć, transport lub aplikacja

6. Numer identyfikacyjny: połączenie lub sesja

7. Ocena: Priorytet lub znaczenie do rozważenia przez procesor

8. Naruszenie: rodzaj naruszenia lub ostrzeżenia

9. Rozmiar: liczba bajtów przesłanych przez połączenie

10. Poświadczenia: nazwa użytkownika, hasło, wszelkie kody specjalne

11. Ładowność: Wymieniane dane na poziomie aplikacji

Techniki wykrywania

Techniki wykrywania włamań można podzielić odpowiednio na trzy kategorie

• Wykrywanie oparte na sygnaturach

• Wykrywanie na podstawie anomalii

• Analiza stanowa protokołu

W wykrywaniu opartym na sygnaturach IDPS ma bazę danych parametrów wskazujących na znanego wirusa. Na przykład, jeśli plik o nazwie miłość. exe jest znany jako wirus, jego obecność wygeneruje alert, a IDPS podejmie odpowiednie działania. Ponadto, jeśli źródło lub miejsce docelowe pakietu ma adres IP z czarnej listy, adres MAC lub międzynarodowy identyfikator urządzenia mobilnego (IMEI), ponownie zostanie wygenerowany alert. Możliwe, że na podstawie adresu IP można umieścić na czarnej liście cały region geograficzny lub utworzyć zasób niedostępny na przykład w godzinach wolnych od pracy. W przypadku wykrywania opartego na sygnaturach używane są czarne listy (gorące listy) i białe listy. Oczywiście wykrywanie oparte na sygnaturach nie jest możliwe w przypadku nieznanych zagrożeń. Czarne listy zawierają sygnatury dyskretnych bytów, które mogą być związane z włamaniami. Takimi jednostkami są hosty, numery portów, aplikacje, nazwy plików lub rozszerzenia plików lub inne wymierne parametry, które można rozpoznać w komunikacji sieciowej. Białe listy zawierają sygnatury dyskretnych bytów które mogą podnieść flagę włamania, podczas gdy w rzeczywistości wiadomo, że są łagodne.

W wykrywaniu opartym na anomaliach IDPS ma bazę danych profili, które reprezentują „normalne" zachowanie sieci. Jeśli coś wydaje się niezwykłe, podnosi się flagę. To jest jak kontrola paszportowa na przejściach międzynarodowych. Jeśli dana osoba jest na czarnej liście lub zauważono coś dziwnego, pojawia się alert. Profile te opisują oczekiwane zachowanie aplikacji, sieci, hostów, a nawet indywidualnych użytkowników. Parametry takich profili mogą być oparte na informacjach statystycznych i mogą się dynamicznie dostosowywać. Oznacza to, że zastosowanie sztucznej inteligencji może pozwolić na stopniową zmianę tych profili bez tworzenia ostrzeżenia. Odchylenie od tych profili zabrzmi alarm i IDPS zajmie odpowiednie działanie. W przypadku wykrywania na podstawie anomalii wymagana jest znaczna ilość dostrajania. Ciasne progi spowodują fałszywe alarmy, natomiast

luźne progi mogą nie rozpoznać złośliwej aktywności. Ataki typu „odmowa usługi" (DoS) można rozpoznać za pomocą sztucznej inteligencji, która monitoruje tempo wzrostu ruchu sieciowego. „Jeśli sztuczna inteligencja jest wbudowana w routery internetowe, routery mogą wspólnie stworzyć internetowy SCADA zdolny do wykrywania i zapobiegania potencjalnym atakom DoS". Jednak „systemy IDS oparte na anomaliach są bardziej podatne na generowanie fałszywych alarmów ze względu na ciągle zmieniający się charakter sieci, aplikacji i exploitów". „Główną zaletą metod wykrywania opartych na anomaliach jest to, że mogą być bardzo skuteczne w wykrywaniu nieznanych wcześniej zagrożeń". W stanowej analizie protokołu opracowywane są modele wydajności protokołu, które służą jako odniesienia nominalne. W pewnym sensie technika ta przypomina wykrywanie oparte na anomaliach, ale zamiast statystycznie budować modele normalnej pracy, tutaj stosuje się profile dostarczone przez dostawcę. „Kiedy przeprowadzamy analizę stanową protokołu, monitorujemy i analizujemy wszystkie zdarzenia w ramach połączenia lub sesji" [6], a następnie mapujemy zachowanie na dostępne profile. Ta technika wykrywania, choć przydatna, nie może wykryć ataków, chyba że nastąpi naruszenie oczekiwanego zachowania.

Działania zapobiegawcze

IDPS, jak sugeruje ich nazwa, po wykryciu oczekuje się, że faktycznie zapobiegnie próbie wtargnięcia. Można to osiągnąć na różne sposoby, w tym

• Blokowanie dostępu do wszystkich usług docelowych zasobów (bazy danych, serwera lub aplikacji).

• Blokowanie wszelkiej komunikacji z użytkownikami posiadającymi określony identyfikator, taki jak adres IP, adres MAC, numer użytkownika lub inne unikalne cechy podejrzanego atakującego.

• Blokowanie dalszej aktywności sesji połączenia sieciowego, które spowodowało incydent.

• Blokowanie tylko zainfekowanej części transakcji. Dotyczy to załącznika do wiadomości e-mail lub toksycznego pliku towarzyszącego plikowi HTML.

• Blokowanie żądania atakującego przez zmianę kryteriów zapory sieciowej.

Jest bardzo możliwe, że IDPS może przegapić atak, tworząc fałsz negatywny lub może zablokować bona fide użytkownika, tworząc fałszywie dodatni. Jednak dzięki szeroko zakrojonym testom wstępnym i dostosowaniu, IDPS może asymptotycznie zbliżyć się do perfekcji.

Zarządzanie IDPS

Po nabyciu IDPS jego zarządzanie dotyczy wdrożenia, działania i utrzymania systemu. Organizacje powstrzymują się od wewnętrznego opracowywania IDPS z dwóch powodów. Jednym z nich jest to, że IDPS, aby był potężny, musi być bardzo złożony. Po drugie, IDPS są łatwo dostępne i można je konfigurować ponownie.

Realizacja

Wdrożenie nabytego produktu IDPS składa się z pięciu etapów.

• Krok pierwszy: identyfikacja funkcji produktu

• Krok drugi: Zaprojektowanie architektury / topologii, w której cechy produktu są odwzorowane na wymagania dotyczące wykrywania włamań i zapobiegania w systemie informatycznym, który ma być chroniony

• Krok trzeci: instalacja IDPS, która może być oprogramowaniem aplikacyjnym lub sprzętowym

• Krok czwarty: Progresywne testowanie IDPS

• Krok piąty: Aktywacja systemu, z możliwym powrotem do dowolnego z kroków

Krok pierwszy: funkcje

Dostępnych jest wiele IDPS. Niektóre mają formę aplikacji. Oznacza to, że IDPS to oprogramowanie o minimalnym kodzie, które szeroko wykorzystuje procedury lub moduły dostępne w systemie operacyjnym hosta i jest oczywiście specyficzne dla systemu operacyjnego. Inne są w formie urządzenia. Oznacza to, że oprogramowanie jest samowystarczalnym pakietem z własnymi procedurami i jest niezależne od systemu operacyjnego hosta.

Krok drugi: architektura

Zaprojektowana architektura zapewni topologię zastosowanego IDPS, biorąc pod uwagę lokalizacje monitorowania i poziom oczekiwanej niezawodności. W celu zwiększenia niezawodności zastosowano redundancję czujników, gdy wiele czujników monitoruje tę samą aktywność. Architektura IDPS zajmuje się także lokalizacją innych komponentów IDPS, takich jak serwery i konsole administracyjne. IDPS połączy się z chronionym przez siebie systemem informatycznym w celu gromadzenia danych i wpływania na niezbędne działania.

Krok trzeci: instalacja

Po zidentyfikowaniu rozwiązania IDPS i zdefiniowaniu topologii instalacja może być kontynuowana. Zazwyczaj urządzenia IDPS oparte na urządzeniach są łatwiejsze do wdrożenia. Najważniejszym parametrem pozostaje jednak ustawienie czujników. W zależności od konkretnej aplikacji bezpieczeństwa czujniki mogą być umieszczone przed lub za zaporami ogniowymi, w krytycznych podsieciach, na serwerach WWW i e-mail oraz w krytycznych bazach danych.

Krok czwarty: testowanie

Testowanie systemu i szkolenie operatora powinny przebiegać równolegle. Testowanie jest długim procesem, podczas którego kryteria wykrywania i zapobiegania są dostosowywane w celu zminimalizowania fałszywych alarmów. Szkolenie operatorów będzie działaniem ciągłym, w miarę wprowadzania nowych zagrożeń i aktualizacji oprogramowania.

Krok piąty: Aktywacja

Jest to ostatni etap, w którym system wchodzi w życie. Praktyka pokazała, że kiedy IDPS jest aktywowany przy wszystkich czujnikach aktywnych jednocześnie, duża liczba fałszywych alarmów przytłacza operatora. Sugeruje się, że aktywacja czujników odbywa się w sposób progresywny, tak aby można było wprowadzić dodatkowe dostrojenie. Stopniowe wdrażanie IDPS najlepiej ujawni ukryte problemy i zmaksymalizuje skuteczną ochronę systemu informatycznego. W fazie aktywacji tymczasowe, częściowe lub całkowite awarie systemu mogą okazać się konieczne do logicznego i fizycznego zaangażowania IDPS w sieć produkcyjną.

Na etapie produkcji konieczna będzie ciągła aktualizacja bazy danych podpisów, a także korekty progów. Biorąc pod uwagę znaczenie IDPS w bezpiecznym działaniu systemu informatycznego, sugeruje się, aby poświadczenia administratorów obejmowały uwierzytelnianie dwuskładnikowe, szczególnie w przypadku korzystania z dostępu zdalnego.

Operacja

Produkty IDPS są zwykle obsługiwane za pomocą konsoli, która wykorzystuje graficzny interfejs użytkownika, a niektóre oferują również interfejs wiersza poleceń. Za pomocą konsoli administrator może wykonywać szeroki zakres czynności, w tym

• Monitorowanie i analiza danych IDPS

• Konfiguracja i aktualizacja parametrów czujnika i serwera zarządzania, w tym segmentacja misji IDPS na sektory, ułatwiając w ten sposób operacje i rozwiązywanie problemów

• Konfiguracja kont użytkowników i parametrów autoryzacji, w tym określone uprawnienia i czujniki do monitorowania

• Projektowanie i przygotowanie harmonogramu, na żądanie i raportowanie wyjątków

Za pomocą konsoli operatorzy mogą definiować, edytować, przechowywać i pobierać zapytania. Można także tworzyć zdefiniowane przez użytkownika filtry zapytań i profile alertów oraz przygotowywać raporty niestandardowe.

Konserwacja

IDPS musi być utrzymywany w sposób ciągły. Oczekiwana konserwacja składa się zasadniczo z trzech części - potwierdzających prawidłowe działanie, aktualizację oprogramowania i szkolenie odpowiedzialnego personelu.

Konserwacja to nieuniknione zadanie - wykonywane online i offline - wpłynie to na oczekiwaną ciągłość usługi. Potwierdzenie prawidłowego działania obejmuje monitorowanie i testowanie. Testowanie może odbywać się okresowo i może odbywać się w środowisku testowym offline lub w trakcie produkcji systemu - w trybie online. Aktualizacja oprogramowania obejmuje aktualizację bazy sygnatur zagrożeń; dostosowanie poziomów zagrożenia; aktualizacja oprogramowania dostarczonego przez dostawcę poprzez instalację poprawek; oraz rekonfigurację systemu, gdy wymagają tego nowe wymagania, technologie i zagrożenia. Po każdej aktualizacji wymagany jest dokładny test. Wskazane jest, aby przed zastosowaniem aktualizacji potwierdzić ich autentyczność za pomocą dostępnych mechanizmów. Zazwyczaj sumy kontrolne plików aktualizacyjnych obliczone przez administratora muszą odpowiadać sumom dostarczonym przez dostawcę. Ponadto tworzenie kopii zapasowych starych konfiguracji jest zawsze dobrym pomysłem. Ciągłe szkolenie odpowiedzialnego personelu jest absolutnie niezbędnym zadaniem w celu rozwijania umiejętności najlepszej obrony systemu. Szkolenie zazwyczaj odbywa się na miejscu, po wstępnym zapewnieniu przez sprzedawcę, aby wszyscy mogli nabrać tempa.

Dokumentacja produktu jest zawsze doskonałym źródłem informacji, na których operatorzy mogą polegać, nie wspominając już o oczekiwanej dostępności wsparcia przez czat na żywo. Skuteczny nadzór i działanie IDPS wymaga specjalistów IT posiadających umiejętności w zakresie bezpieczeństwa informacji i administracji sieci, a także administracji systemem, na których można budować swoją stale rosnącą wiedzę w zakresie bezpieczeństwa cybernetycznego z naciskiem na włamania, wykrywanie i zapobieganie. W tym celu wskazane jest dołączenie do grupy użytkowników danego produktu, ponieważ służy on jako forum gdzie pojawiają się problemy i obawy i, miejmy nadzieję, znajdują rozwiązania. Aby skoncentrować się na swojej podstawowej działalności, wiele organizacji zleca bezpieczeństwo swojego systemu informatycznego firmom poświęconym tej dziedzinie z dużym doświadczeniem i wiedzą specjalistyczną. Oczywiście outsourcing musi być oceniany pod kątem misji i ograniczeń organizacji.

Klasyfikacja IDPS

IDPS są podzielone na następujące cztery ogólne kategorie. Oparty na hoście, który analizuje zdarzenia wewnątrz określonego hosta (komputera) w poszukiwaniu działań, które mogą sugerować włamanie. Oparty na sieci, który analizuje aktywność protokołu w określonej sieci (urządzeniach lub segmentach) w poszukiwaniu nieprawidłowości protokołu Network Behavior, który analizuje zdarzenia, które mogą ujawnić zasady naruszenia, obecność złośliwego oprogramowania lub rozproszona odmowa usługi. Bezprzewodowy, który sprawdza ruch sieci bezprzewodowej podejrzane działania

IDPS oparty na hoście

IDPS oparty na hoście jest systemem wykrywania i zapobiegania włamaniom który dotyczy pojedynczego hosta, to znaczy jednej stacji roboczej lub serwera (sieć, e-mail, DNS lub inny). Zazwyczaj ten IDPS monitoruje następujące sześć obszarów i działań:

• Zewnętrzny interfejs przewodowy

• Bezprzewodowy (Wi-Fi i Bluetooth)

• Ruch modemowy

• Status pliku (dostęp, modyfikacja i tworzenie)

• Konfiguracja systemu (statyczna lub dynamiczna)

• Uruchamianie procesów (zarówno systemowych, jak i aplikacji)

Obserwacje w powyższych obszarach są porównywane z szablonami oczekiwanej wydajności i może powodować alerty wykrywania i / lub działania zapobiegawcze.

IDPS oparty na hoście może być oparty na oprogramowaniu, w którym to przypadku jest instalowany wewnątrz samego monitorowanego hosta, lub może być oparty na urządzeniu, w którym to przypadku jest oddzielnym fizycznym elementem sprzętowym umieszczonym w linii między monitorowanym hostem a ścieżka do Internetu lub intranetu. W przypadku aplikacji istnieją dwa podejścia: jedno, gdzie agent monitoruje wyniki działań, a drugi, w których część kodu (zwana shims) jest wstawiany w wybrane miejsca, takie jak system operacyjny, kod systemu operacyjnego, kod aplikacji lub protokoły, służąc jako mini-zapory ogniowe zdolne do wykrywania i blokowania niepożądanej aktywności. W przypadku urządzenia urządzenie jest fizycznie poza hostem i nie ma możliwej mikrokontroli zapewnionej przez podkładki, ale jest niezależne od zastosowanego systemu operacyjnego. Rejestrowane parametry wykrytych zdarzeń obejmują

• Rodzaj zdarzenia i jego priorytet.

• Znacznik czasu na podstawie przypisanego źródła. Większość IDPS generuje własne znaczniki czasu zamiast kopiować je z zewnętrznego źródła.

• Powiązane adresy portów i IP (Internet i intranet).

• Nazwy plików i ich ścieżki (katalogi, podkatalogi itp.).

• Poświadczenia autoryzacji / uwierzytelnienia (nazwy użytkowników).

Host IDPS sprawdza kody pod kątem złośliwego oprogramowania, wykonując je w środowisku piaskownicy, to znaczy w środowisku, w którym wykonanie nie może zaszkodzić innym programom, ani nie może wykorzystywać zabronionych zasobów. W tym nadzorowanym wykonaniu agent IDPS szuka

• Naruszenia, takie jak zapuszczanie się w nieautoryzowane miejsce

• Eskalacja uprawnień

• Przepełnienie bufora, stos lub stos

• Nieautoryzowane wywołania biblioteki

• Sekwencje instrukcji, które mogą być albo kopiowaniem klawiszy, albo próbą instalacji rootkitów

IDPS oparty na hoście sprawdza również integralność, właściwości i dostęp do plików. Integralność jest sprawdzana za pomocą testu sumy kontrolnej; jeśli jest niepoprawny, oznacza to, że zawartość pliku została zmieniona. Suma kontrolna jest resztką, resztką, sekwencją binarną powstałą po przejściu zawartości pliku przez z góry określony algorytm. Właściwości pliku są bardzo ważne dla bezpieczeństwa i integralności zawartości pliku. Właściwości obejmują uprawnienia dostępu - odczyt / zapis, autorstwo pliku, znaczniki czasu dostępu i modyfikacji, podpis cyfrowy i ewentualnie inne parametry w zależności od typu pliku. Kontrola dostępu do plików jest najważniejszą funkcją bezpieczeństwa. Umieszczenie podkładki dystansowej może wykryć naruszenia zasad, a nawet wdrożyć zasady bezpieczeństwa poprzez blokowanie dostępu. IDPS oparty na hoście, podobnie jak inne systemy, wymaga strojenia. Musi to mieć miejsce przy początkowej aktywacji, a także po instalacji lub wymianie wybranych chronionych plików. Ponadto, białe i czarne listy muszą być aktualne, aby zapobiec fałszywym wykryciom. Przed wdrożeniem konflikt z innymi systemami ochrony musi zostać rozwiązany, aby uniknąć nieprawidłowego działania w obu systemach. Z powodu ciągłej czujności IDPS oparte na hoście stanowią obciążenie dla chronionego hosta, wymagając znacznego czasu procesora i miejsca w pamięci i dysku. Ponadto między instalacją a wdrożeniem wymagane są szeroko zakrojone testy w celu zapewnienia poprawnej integracji IDPS z hostem. Takie testy będą musiały odbywać się w trybie offline, co spowoduje, że host będzie nieczynny w tym okresie.

IDPS oparty na sieci

W sieci IDPS czujniki mogą być aplikacjami lub urządzeniami i mogą monitorować więcej niż jedno urządzenie lub segment w sieci. Aby zastosować środki zapobiegawcze, czujniki muszą być zainstalowane w linii. Czujniki liniowe muszą mieć bardzo dużą prędkość, aby nie powodowały zatorów komunikacyjnych. Jeśli obsługa ruchu osiągnie punkt prawie nasycenia, ruch musi przepuścić niezaznaczony lub ruch o niskim priorytecie zostać zrzucony, aby zmniejszyć obciążenie. W przypadku instalacji pasywnej obserwacje są zgłaszane tylko bez możliwości blokowania wykrytych zdarzeń. Czujniki pasywne przekazują zebrane dane do serwera zarządzania, gdzie są analizowane i gdzie można podjąć działania zapobiegawcze.Sieciowe IDPS z czujnikami wbudowanymi mogą interweniować i zapobiegać próbom wykonania zdarzenia, podczas gdy sieciowe IDPS z pasywnymi czujnikami służą jedynie jako obserwatorzy i reporterzy zdarzeń. IDPS oparte na sieci analizują działania w warstwach sieci, transportu i aplikacji, a większość wykorzystuje wszystkie trzy techniki wykrywania omówione wcześniej , a mianowicie wykrywanie oparte na sygnaturach, wykrywanie oparte na anomalii i analizę stanowego protokołu. Procesy wykrywania można rozdzielić na kilka czujników obsługiwanych przez moduł równoważenia obciążenia IDPS. IDPS oparty na sieci jest w zasadzie obserwatorem obserwującym przepływający ruch sieciowy. W tym procesie IDPS poszukuje naruszeń, zgodnie z ustalonymi kryteriami. IDPS zgłasza takie naruszenia na odpowiednim serwerze zarządzania IDPS, który może zastosować środki zapobiegawcze. Rodzaje gromadzonych danych obejmują adresy IP i MAC komunikujących się hostów, a także typ i wersję systemu operacyjnego. Ustalenie wersji prowadzi do informacji o istnieniu możliwych luk, które należy chronić. Inne zebrane parametry to liczba używanych portów, aplikacji i ich wersji, liczba przeskoków w podróży między dwoma hostami oraz inne dane, które normalnie są zawarte w protokołach komunikacyjnych.

System analizy zachowania sieci

System analizy zachowań sieci (NBA), jak sama nazwa wskazuje, bada zachowanie skończonej sieci i zwykle jest oparty na urządzeniach. NBA biernie obserwuje liczne punkty i działania protokołów w sieci i tworzy punkt odniesienia, który stale się aktualizuje i stanowi „normalne zachowanie w ruchu". NBA wykorzystuje ten model jako punkt odniesienia do wykrywania odchyleń, a także do rozpoznawania trendów w korzystaniu z różnych zasobów. NBA idealnie nadaje się do wykrywania ataków DoS lub ciągłych prób łamania kodów autoryzacyjnych. Czujnik NBA może być instalowany w trybie, w linii lub pasywny. W trybie in-line NBA służy jako minifirewall, blokując żądania od podejrzanych hostów. W trybie pasywnym NBA zbiera dane z podsłuchiwanego ruchu - takie jak adresy IP komunikujących się hostów, używane protokoły i aktywne aplikacje - i interweniuje w razie potrzeby, przerywając połączenia, które wspierają działania, którym nie można ufać. Rycina 7.8 ilustruje topologię systemu wykrywania włamań NBA.

Bezprzewodowe IDPS

Bezprzewodowy IDPS monitoruje wydajność bezprzewodowych sieci lokalnych (WLAN). Faktyczną technologią WLAN jest Wi-Fi, oficjalnie znany jako IEEE 802.11. Ta technologia działa w widmach podzielonych na kanały, w których komunikacja nieustannie zmienia kanały. Dlatego bezprzewodowy IDPS powinien mieć jeden czujnik na kanał, aby zmaksymalizować jego wydajność. Jeśli jest tylko jeden czujnik, czujnik ten będzie musiał przeskakiwać z kanału na kanał, naturalnie tracąc aktywność na drodze. Bezprzewodowe IDPS mogą być autonomiczne lub osadzone w bezprzewodowym punkcie dostępowym (AP), skąd monitorują aktywność sieci. Mimo że technologia Wi-Fi zapewnia bezpieczeństwo danych za pośrednictwem WEP (Wired Equivalent Privacy), jej siła szyfrowania jest uważana za słabą i podatną na złamanie i konieczne są dodatkowe środki. Nawet jeśli organizacja nie ma działającej sieci bezprzewodowej, można wdrożyć bezprzewodowy IDPS, aby zbadać fale radiowe i upewnić się, że żaden nieautoryzowany punkt dostępowy nie jest podłączony do sieci organizacji. Jako minimum należy użyć wyszukiwarki Wi-Fi, aby potwierdzić, że żaden nieautoryzowany punkt dostępowy nie jest podłączony w sieci LAN organizacji. Rysunek 7.10 pokazuje typową wyszukiwarkę Wi-Fi. Jeśli organizacja rzeczywiście ma działające sieci WLAN, „Obecnie dostępne są rozwiązania, w których pozycjonowanie czujników RF może geometrycznie ustalić, czy klient znajduje się w autoryzowanym obszarze fizycznym. Takie technologie, które wymagają szkolenia w terenie i dokładnego dostrojenia, zapewniają 100% bezpieczeństwa podczas testów ". Rozmieszczenie czujników musi uwzględniać różne czynniki, w tym:

• Zasięg czujników i plan piętra budynku

• Topologia bezprzewodowych punktów dostępowych organizacji

• Topologia przewodowej sieci organizacji

• Koszt IDPS a wartość chronionych danych

• Fizyczne bezpieczeństwo urządzeń

• Zastosowane technologie IDPS

Wykryte zdarzenia są oceniane w odniesieniu do kryteriów podobnych do kryteriów pozostałych trzech typów IDPS opisanych powyżej. Oczekiwane możliwości bezprzewodowego IDPS obejmują:

• Rozpoznanie obecności wszystkich urządzeń bezprzewodowych-punktów dostępowych lub stacji.

• Określenie fizycznej lokalizacji dowolnego urządzenia bezprzewodowego - AP lub stacji. Znalezienie fizycznej lokalizacji odbywa się poprzez triangulację, która będzie wymagać zastosowania kilku czujników.

• Uznanie naruszeń zasad.

• Możliwość wykonania akcji zapobiegawczej, gdy wciąż jest w trybie wykrywania. Odbywa się to za pomocą dwóch niezależnych modułów RF, jeden nasłuchuje cały czas, a drugi przesyła informacje o zdarzeniach.

• Wykrywanie obecności

• Ataki typu man-in-the-middle

• Ataki DoS

• Skanery sieci bezprzewodowej używane przez wardrivers (Wardrivers to osoby, które jeżdżą po ulicach, aby zlokalizować sieć bezprzewodową do użycia lub ataku.

Rejestrowane parametry wykrytych zdarzeń obejmują:

• Identyfikacja numeru MAC lub IMEI urządzenia bezprzewodowego podejrzewanego o zdarzenie.

• Liczba kanałów, przez które miało miejsce wydarzenie.

• Adres intranetowy przypisany do urządzenia bezprzewodowego przez AP. Zazwyczaj jest to adres 192.168.1.xx, gdzie xx to numer przypisany do urządzenia.

• Znacznik czasu na podstawie przypisanego źródła. Większość IDPS generuje własne znaczniki czasu zamiast kopiować je z zewnętrznego źródła.

• Rodzaj zdarzenia i poziom priorytetu według klasyfikacji IDPS.

• Numer czujnika, jeżeli należy zastosować wieloczujnikowy IDPS.

• Rodzaj zastosowanych środków zaradczych. Zazwyczaj zakończenie połączenia i zapobieganie nowemu połączeniu z podejrzaną jednostką.

Wstępne wdrożenie bezprzewodowego IDPS wymaga inicjalizacji, w której wprowadzane są parametry legalnych jednostek i przeprowadzane jest dostrajanie, aby upewnić się, że chroniony teren jest odpowiednio objęty.

Przewidywanie ataków cyberbezpieczeństwa

Przyspieszenie ataków cyberbezpieczeństwa umożliwiło ostrożnym obserwatorom dokonywanie prognoz, z których większość niestety się sprawdziła. Predyktorzy opracowali algorytmy - metodologie - w których komponenty wejściowe obejmują dogłębną znajomość organizacji

• Umiejętności na poziomie C-Suite

• Umiejętności w maszynowni IT

• Konfiguracja systemu informacyjnego

• Operacje biznesowe

• Plan ciągłości działania

• Zależność od podmiotów zewnętrznych

Ponadto w tym algorytmie predykcyjnym wprowadzono aktualny i prognozowany stan techniki szkodliwego oprogramowania. Wiedza uzyskana z tych ćwiczeń pomaga lepiej zrozumieć organizację

• Filozofia cyberbezpieczeństwa

• Obszary krytyczne w stosunku do celów organizacyjnych

• Narażenie na cyberbezpieczeństwo

• Następstwa poważnego cyberataku

• Możliwe możliwości cyberobrony

Analizy, takie jak powyższe, powinny być przeprowadzane w organizacji raz w roku, jeśli nie w sposób ciągły, przy czym oprócz oceny zdolności obronnych pierwszej linii należy zaprojektować i przetestować tworzenie kopii zapasowych danych oraz redundancję operacyjną / funkcjonalną. Zazwyczaj taka samoocena cyberbezpieczeństwa składa się z czterech części, a mianowicie:

• Podstawowa konfiguracja zabezpieczeń systemu, w której narzędzia oceny ryzyka ujawniają luki, które należy wyeliminować lub zminimalizować.

• Modelowanie, symulacja i analiza, w których symulowane są wektory ataków i oceniana jest ekspozycja cybernetyczna.

• Demonstracja podatności, w której rzeczywiste testy penetracyjne są stosowane w systemie, oceniając jego działanie w warunkach pożaru na żywo.

• Alokacja działań naprawczych i ryzyka rezydualnego, w których dokonuje się ustalania priorytetów ryzyka i przydzielane są środki zaradcze, w zależności od tego, jak krytyczny może być niekorzystny wpływ.

Biorąc pod uwagę, że na cyber bitewnym polu broń ofensywna nie jest jak dotąd ani znana, ani znormalizowana, nie należy się spodziewać podatności na zero dni, a dzięki odpowiednim redundancjom i lustrzanym bazom danych obrażenia cybernetyczne zostaną zminimalizowane.

Trendy w zakresie cyberbezpieczeństwa

Konfrontacja w zakresie cyberbezpieczeństwa podlega dwustopniowej ewolucji, a mianowicie cyberatakom prowadzącym scenę i cyberobrony, która się rozwija. W atakach cybernetycznych tradycyjne ataki, takie jak rozproszona odmowa usługi (DDoS), maleją, a liczba ransomware rośnie i rośnie. Niestety dostępność waluty internetowej, takiej jak BitCoin, ułatwia anonimową płatność żądanego okupu. Przewiduje się, że korzystanie z urządzeń Internetu Rzeczy w krytycznych aplikacjach przyciągnie Ransomware-of-Things (RoT) w celu ich zainfekowania, utrzymując ich unikalną operację w niewoli do momentu zrealizowania niemożliwej do wykrycia płatności. W cyberobronie ośmioznakowe hasło jest zastępowane wieloskładnikowym, zwykle dwuskładnikowym schematem autoryzacji, przy czym jeden ma charakter biometryczny. Ponadto wykorzystanie szyfrowania wzrosło wraz ze wzrostem świadomości cyberbezpieczeństwa. Obserwuje się także trend wzrostu edukacji w zakresie bezpieczeństwa cybernetycznego, prowadzący do uzyskania certyfikatów i stopni uniwersyteckich. Jednak zapotrzebowanie nie jest zaspokojone, co powoduje nadmierną liczbę subskrybowanych programów