BEZPIECZEŃSTWO ZA ZAPORĄ.

Nawet dzisiaj, gdy zapytano ich, jak zabezpieczyliby komputer lub sieć komputerową, większość ludzi wspomina o zaporach ogniowych, pierwszych powszechnie akceptowanych urządzeniach zabezpieczających sieć. Ponieważ bezpieczeństwo sieci stało się nieobowiązkowym aspektem zarządzania systemem, różnego rodzaju mechanizmy zapory ogniowej stały się standardem w wielu sieciach. Podobnie jak w przypadku każdej złożonej funkcji ochrony, zapory są konieczne, ale nie wystarczają, aby całkowicie chronić przedsiębiorstwa przed naruszeniami bezpieczeństwa. Oczekiwanie, że zapory ogniowe zapewnią pełną ochronę, jest równoznaczne z oczekiwaniem, że strażnicy przy bramach kampusów korporacyjnych zapobiegną destruktywnemu zachowaniu ze strony pojazdów obsługujących obiekt. nawet przedmioty, które wydają się niegroźne dla strażników, mogą zostać wykorzystane do przenoszenia niszczycielskich ładunków. Dlatego większość nowoczesnych architektur bezpieczeństwa sieci obejmuje systemy wykrywania włamań i zapobiegania włamaniom. Systemy wykrywania włamań (IDS) to systemy programowe lub sprzętowe, które automatyzują monitorowanie zdarzeń występujących w systemie komputerowym lub sieci. IDS nie tylko gromadzą i synchronizują zapisy tych zdarzeń; analizują je również pod kątem oznak naruszenia bezpieczeństwa. Mówiąc najściślej, systemy oceny podatności (VAS) to specjalna klasa systemów IDS, w których system opiera się na statycznej inspekcji i odtwarzaniu ataków w celu oceny narażenia systemu docelowego na określone luki w zabezpieczeniach. Systemy zapobiegania włamaniom (IPS) to kolejna specjalna klasa systemów wykrywania włamań, w których system jest zaprojektowany do reagowania na określone wykryte ataki w określony z góry sposób. W ostatnich latach dziedzina wykrywania włamań poszerzyła się i pogłębiła, napędzana wieloma czynnikami. Pracownicy ochrony, zarówno architektoniczni, jak i operacyjni, zdobyli większe doświadczenie w zakresie technologii IDS, współpracując z komercyjnymi dostawcami produktów w celu rozszerzenia możliwości produktów i schematów zarządzania, aby dopasować je do aktualnych potrzeb. Ponieważ personel operacyjny stał się bardziej komfortowy w korzystaniu z tych systemów, przeniósł pewne możliwości IDS do centrów zarządzania siecią. Wreszcie, zagrożenia ewoluowały, napędzając potrzeby, którym IDS mają wyjątkowe kwalifikacje. Ewolucja IDS spowodowała pewne zmiany w nazewnictwie i związanym z nim rzemiośle. Jedną z tych zmian jest to, że ocena podatności jest uważana za odrębną dyscyplinę, napędzaną potrzebami rynku, które często różnią się od tych, które mają wpływ na IDS. Innym powodem jest to, że zapobieganie włamaniom wyewoluowało jako samodzielna kategoria produktów, oferująca możliwość automatycznego reagowania na określone klasy ataków.

Co to jest wykrywanie włamań?

Wykrywanie włamań to proces zbierania informacji o zdarzeniach zachodzących w systemie komputerowym lub sieci i analizowania ich pod kątem oznak włamań. Włamania są definiowane jako naruszenia zasad bezpieczeństwa, zwykle charakteryzowane jako próby naruszenia poufności, integralności lub dostępności komputera lub sieci. Naruszenia te mogą pochodzić od ataków uzyskujących dostęp do systemów z Internetu lub od upoważnionych użytkowników systemów, którzy próbują przekroczyć swoje uprawnione poziomy uprawnień lub którzy wykorzystują swój legalny dostęp do systemu w celu prowadzenia nieautoryzowanej działalności. Systemy wykrywania włamań to oprogramowanie lub sprzęt, które automatyzują ten proces monitorowania i analizy.

Co to jest zapobieganie włamaniom?

Zapobieganie włamaniom to proces łączenia wykrywania włamań (zgodnie z definicją) z określonymi reakcjami na pewne wykryte scenariusze włamań. Zdarzenia wyzwalające mogą być postrzegane jako szczególny podzbiór włamań i często charakteryzują się bogatszymi kategoriami ilościowymi i jakościowymi niż bardziej ogólne wyzwalacze IDS. Na przykład określony IPS może skupiać się na

monitorowaniu określonych typów ruchu sieciowego. Gdy prędkość określonego typu ruchu przekroczy spodziewany próg, IPS zareagowałby w określony z góry sposób (np. Ograniczając szybkość kolejnego ruchu tego typu).

Gdzie wykrywanie włamań i zapobieganie włamaniom mieszczą się w zarządzaniu bezpieczeństwem?

Wykrywanie włamań jest niezbędną funkcją większości strategii bezpieczeństwa systemu. To (i jej pochodna, ocena podatności) jest podstawową technologią bezpieczeństwa, która wspiera cel, jakim jest audytowalność. „Możliwość audytu" oznacza zdolność do niezależnego przeglądania i sprawdzania zapisów i działań systemowych w celu:

* Określić adekwatność kontroli systemu

* Zapewnij zgodność z ustaloną polityką bezpieczeństwa i procedurami operacyjnymi

* Wykrywaj naruszenia bezpieczeństwa

* Zaproponuj wszelkie wskazane zmiany

Z kolei obecność silnej funkcji audytu umożliwia i wspiera kilka ważnych funkcji zarządzania bezpieczeństwem, takich jak obsługa incydentów i odzyskiwanie systemu. Wykrywanie włamań pozwala również menedżerom ds. Bezpieczeństwa na elastyczne sposoby dostosowywania się do potrzeb użytkowników, zachowując jednocześnie zdolność do ochrony systemów przed określonymi typami zagrożeń. Trwa dyskusja na temat tego, czy IPS wyprze IDS w składzie zarządzania bezpieczeństwem. To przemieszczenie jest na razie mało prawdopodobne ze względu na powiązania między IDS a audytem. Ponieważ operacje bezpieczeństwa stają się ściślej zintegrowane z tradycyjną administracją i operacjami systemu, funkcje audytowe są niezbędne do wspierania analizy przyczyn źródłowych w diagnozowaniu i usuwaniu awarii systemu. Źle dostrojone urządzenia zabezpieczające mogą powodować problemy w działaniu; ważne jest, aby móc szybko i właściwie zidentyfikować i skorygować takie problemy. Funkcje audytowe są również niezbędne do pomiaru skuteczności środków bezpieczeństwa w ograniczaniu zagrożeń bezpieczeństwa. Chociaż może się wydawać, że przejrzyste wykrywanie i blokowanie ataków jest optymalnym procesem bezpieczeństwa, taka przejrzystość - czyli brak ścieżki audytu - koliduje z wykazaniem skuteczności środków bezpieczeństwa wobec rzeczywistych zagrożeń. Innymi słowy, aby zarządzanie bezpieczeństwem uzasadniało budżet na środki bezpieczeństwa, musi być w stanie udokumentować i określić ilościowo przydatność i skuteczność takich środków. Dlatego, niezależnie od skuteczności IPS w blokowaniu ataków, IDS prawdopodobnie zawsze będzie konieczne do obsługi tych funkcji audytowych. IDS dostarcza podstawowych informacji na temat profili i częstotliwości ataków, które pozwalają menedżerom wykazać skuteczność i zwrot z inwestycji w mechanizmy prewencyjne. Bez twardych dowodów na częstotliwość ataków, menedżerowie ds. Bezpieczeństwa pozostają w pozycji mężczyzny machającego martwym kurczakiem wokół głowy stojąc na rogu ulicy. Zapytany, dlaczego to robi, odpowiada: „Aby trzymać z daleka latające słonie". „Ale nie ma latających słoni" - protestują obserwatorzy. "Widzieć? To działa!" - odpowiada wariat. Chociaż systemy wykrywania i zapobiegania włamaniom są niezbędne jako funkcje bezpieczeństwa systemu, nie są one wystarczające do ochrony systemów przed wszystkimi zagrożeniami. IDS i IPS muszą być częścią bardziej kompleksowej strategii bezpieczeństwa, która obejmuje ocenę podatności, politykę bezpieczeństwa i kontrole proceduralne, zapory sieciowe, silne mechanizmy identyfikacji i uwierzytelniania, mechanizmy kontroli dostępu, szyfrowanie plików i łączy, sprawdzanie integralności plików, fizyczne środki bezpieczeństwa, i szkolenia w zakresie bezpieczeństwa.

Krótka historia wykrywania włamań.

Wykrywanie włamań to automatyzacja ręcznych procesów zapoczątkowanych w pierwszych dniach przetwarzania danych. Joseph Wassermann z Bell Telephone Company udokumentował pochodzenie audytu systemu i bezpieczeństwa już w połowie lat pięćdziesiątych, kiedy projektowano i wdrażano pierwszy skomputeryzowany system biznesowy. Możliwość audytowania była kluczową funkcją bezpieczeństwa od najwcześniejszych dni bezpieczeństwa komputerowego, zgodnie z propozycją badania J. P. Andersona z 1973 r., Zleconego przez Siły Powietrzne Stanów Zjednoczonych. Anderson zaproponował schemat automatyzacji przeglądu ścieżek audytu bezpieczeństwa w 1980 r. W raporcie badawczym uważanym przez wielu za przełomową pracę w zakresie wykrywania włamań. Dorothy Denning i Peter Neumann prowadzili badania nad wykrywaniem włamań, prowadzone w latach 1984–1986, tworząc w 1986 r. Kolejną przełomową pracę dotyczącą wykrywania włamań, w której Denning zaproponował model wykrywania włamań. Instancja modelu wykrywania włamań Denninga została opracowana jako system ekspercki wykrywania włamań (IDES) przez zespół z SRI International. IDES był systemem hybrydowym, który konstruował profile statystyczne zachowań użytkowników na podstawie dzienników kontroli jądra systemu operacyjnego i innych źródeł danych systemu. IDES dostarczył również system ekspercki oparty na regułach, który umożliwiał użytkownikom określanie wzorców zdarzeń do oznaczania jako włamania. IDES i system następnej generacji IDES (NIDES), który nastąpił po nim, zapoczątkowały erę, w której opracowano wiele projektów badawczych i prototypowych systemów wykrywania włamań, w tym Haystack (Haystack Labs i US Air Force), NADIR (Los Alamos National Laboratory), Wisdom i Sense (Los Alamos National Laboratory i Oak Ridge National Laboratory), ISOA (PRC, Inc.), TIM (Digital Equipment Corporation), ComputerWatch (AT&T) i Discovery (TRW, Inc). Pod koniec lat osiemdziesiątych naukowcy z Uniwersytetu Kalifornijskiego w Davis zaprojektowali pierwszy sieciowy system wykrywania włamań (początkowo nazywany Network Security Monitor, ale później przemianowany na NID), który działał tak samo, jak wiele obecnych komercyjnych włamań sieciowych. produkty do wykrywania. Kolejny produkt badawczy finansowany przez siły powietrzne USA, zwany Distributed Intrusion Detection System (DIDS), badał koordynację sieciowych i hostowych systemów wykrywania włamań. DIDS został opracowany przez zespoły z University of California, Davis, Haystack Laboratories i Lawrence Livermore National Laboratory. Zapobieganie włamaniom zostało zaproponowane jako logiczny kolejny krok w kierunku wykrywania włamań niemal od samego początku badań nad wykrywaniem włamań. Wsparcie dla niektórych modeli zapobiegania włamaniom wzrosło, gdy obawy dotyczące ataków na infrastrukturę sieci TCP / IP (np. Zalewanie pakietów i zniekształcone ataki pakietowe) wzrosły w połowie i pod koniec lat 90. Zaproponowano inne typy IPS, aby radzić sobie z hackami na poziomie jądra i problemami z wyciekiem informacji.

GŁÓWNE POJĘCIA

Kilka strategii stosowanych w wykrywaniu włamań służy do opisu i rozróżnienia określonych systemów wykrywania włamań. Mają one wpływ na zagrożenia, na które reaguje każdy system i często określają środowiska, w których należy używać określonych systemów. Jak zauważono, zapobieganie włamaniom opiera się przede wszystkim na strategiach wykrywania włamań; w związku z tym czynniki różnicujące zostaną odpowiednio wyróżnione.

Struktura procesu.

Wykrywanie włamań definiuje się jako proces monitorowania i generowania alarmów i jako takie można je opisać za pomocą prostego modelu procesu. Model ten jest tutaj naszkicowany i zostanie użyty do zilustrowania podstawowych koncepcji wykrywania włamań.

Źródła informacji.

Pierwszy etap procesu wykrywania włamań obejmuje jedno lub więcej źródeł informacji, zwanych także generatorami zdarzeń. Źródła informacji do wykrywania włamań można podzielić na kategorie według lokalizacji: sieć, host lub aplikacja.

Silnik analizy

Zebrane informacje o zdarzeniu przechodzą do kolejnego etapu procesu wykrywania włamań, w którym są analizowane pod kątem objawów ataku lub innych problemów związanych z bezpieczeństwem.

Odpowiedź

Gdy silnik analizy diagnozuje ataki lub problemy z bezpieczeństwem, informacje o tych wynikach są ujawniane na etapie reakcji procesu wykrywania włamań. Odpowiedzi obejmują szerokie spektrum możliwości, od prostych raportów lub dzienników po automatyczne odpowiedzi, które zakłócają trwające ataki. Obecność tych automatycznych odpowiedzi definiuje system zapobiegania włamaniom.

Podejście do monitorowania

Pierwszym głównym klasyfikatorem używanym do rozróżniania systemów wykrywania włamań jest podejście do monitorowania systemu. Monitorowanie polega na zbieraniu danych o zdarzeniach ze źródła informacji, a następnie przekazywaniu tych danych do silnika analitycznego. Podejście do monitorowania opisuje perspektywę, z której przeprowadzane jest monitorowanie wykrywania włamań. Podstawowe metody monitorowania stosowane obecnie w systemach wykrywania włamań są oparte na sieci, hostach i aplikacjach.

Architektura wykrywania włamań

Nawet na początku ręcznego audytu bezpieczeństwa badacze zauważyli, że aby informacje audytowe były zaufane, powinny być przechowywane i przetwarzane w środowisku innym niż monitorowane. Wymóg ten ewoluował i obejmuje większość podejść do wykrywania włamań z trzech powodów:

1. Aby uniemożliwić intruzowi zablokowanie lub unieważnienie systemu wykrywania włamań poprzez usunięcie źródeł informacji

2. Aby uniemożliwić intruzowi zakłócenie działania czujnika wtargnięcia w celu zamaskowania obecności intruza

3. Zarządzanie wydajnością i obciążeniem pamięci masowej, które może wynikać z uruchamiania zadań wykrywania włamań w systemie operacyjnym

W tej architekturze system, w którym działa system wykrywania włamań, nazywany jest hostem. Monitorowany system lub sieć nazywany jest celem.

Częstotliwość monitorowania

Innym częstym deskryptorem podejść do wykrywania włamań jest czas gromadzenia i analizy danych o zdarzeniach. Zwykle dzieli się to na podejście wsadowe (znane również jako interwałowe) i ciągłe (znane również jako podejście w czasie rzeczywistym). W analizie wsadowej dane o zdarzeniach ze źródła informacji są przekazywane do silnika analizy w postaci pliku lub innego bloku. Jak sama nazwa wskazuje, zdarzenia odpowiadające danemu przedziałowi czasu są przetwarzane (i dostarczane użytkownikowi) po włamaniu. Ten model był najczęściej używany do wczesnego wykrywania włamań, ponieważ zasoby systemowe nie pozwalały na monitorowanie lub analizę w czasie rzeczywistym. W analizie w czasie rzeczywistym dane o zdarzeniach ze źródła informacji są przekazywane do silnika

analitycznego w miarę gromadzenia informacji. Informacje są analizowane natychmiast, dając użytkownikowi możliwość zareagowania na wykryte problemy wystarczająco szybko, aby wpłynąć na wynik włamania.

Strategia analizy

W przypadku wykrywania włamań istnieją dwie przeważające strategie analizy: wykrywanie nadużyć i wykrywanie anomalii. W przypadku wykrywania nadużyć silnik analizy filtruje strumienie zdarzeń, dopasowując wzorce aktywności, które charakteryzują znany atak lub naruszenie bezpieczeństwa. W przypadku wykrywania anomalii silnik analityczny wykorzystuje techniki statystyczne lub inne techniki analityczne, aby wykryć wzorce odpowiadające nieprawidłowemu użytkowaniu systemu. Wykrywanie anomalii opiera się na założeniu, że włamania znacznie różnią się od normalnej aktywności systemu. Ogólnie rzecz biorąc, wtargnięcie w systemy wykrywania polega w większym stopniu na wykrywaniu anomalii i pomiarach ilościowych w celu wykrywania i blokowania ataków.

ZAPOBIEGANIE WŁAMANIU

Jak wspomniano, IPS są często uważane za specjalny przypadek IDS, w którym określone są automatyczne odpowiedzi. Jednak wraz z przyjęciem pierwszej generacji produktów sieciowych IPS ewoluowały dodatkowe specyfikacje dla IPS oprócz specyfikacji przypisanych do IDS.

Architektura systemu zapobiegania włamaniom

Podobnie jak w przypadku wykrywania włamań, większość systemów IPS oddziela platformę monitorowania i analizy od monitorowanej platformy docelowej. Wprowadzono dodatkowe rozróżnienia między tymi IPS, które oddzielają platformę monitorowania i analizy od platformy odpowiedzi (są one oznaczone jako „samodzielne" IPS) i tymi, które integrują wszystkie funkcje w pojedynczej jednostce, zwykle zaporze, przełączniku sieciowym lub routerze (są one oznaczone jako „zintegrowane" IPS).

Strategia analizy zapobiegania włamaniom

IPS generalnie używają tego samego strukturalnego podejścia do analizy danych, co IDS, ale nomenklatura strategii analizy jest inna. Schematy analizy IPS dzielą się na dwie ogólne kategorie, oparte na stawkach i oparte na treści. Analiza IPS oparta na szybkościach podejmuje decyzję o zablokowaniu ruchu sieciowego na podstawie wskaźników obciążenia sieci, mierzonych na podstawie statystyk, takich jak szybkości i liczba połączeń. Ta kategoria analizy jest szczególnie przydatna do wykrywania ataków typu „odmowa usługi" (DDoS). Analiza IPS oparta na zawartości podejmuje decyzję o blokowaniu ruchu sieciowego na podstawie wskaźników anomalnych pakietów i określonej zawartości (często reprezentowanej jako sygnatury IDS). To podejście jest przydatne do wykrywania nieprawidłowo sformułowanych pakietów DDoS i innych typów ataków, których nie można łatwo wykryć za pomocą miar ilościowych

ŹRÓDŁA INFORMACJI

Źródła informacji stanowią pierwszy etap procesu wykrywania włamań. Dostarczają informacji o zdarzeniach z monitorowanych systemów, na podstawie których proces wykrywania włamań opiera swoje decyzje. Źródła informacji obejmują zarówno surowe dane o zdarzeniach (np. Dane zebrane bezpośrednio z mechanizmów audytu systemu i rejestrowania), jak i dane wyjściowe przez narzędzia do zarządzania systemem (np. Narzędzia do sprawdzania integralności plików, narzędzia do oceny podatności, systemy zarządzania siecią, a nawet inne systemy wykrywania włamań). W tej sekcji źródła informacji do wykrywania włamań są klasyfikowane według lokalizacji: sieć, host lub aplikacja.

Monitorowanie sieci

Najpopularniejszym podejściem do monitorowania wykorzystywanym w systemach wykrywania włamań jest sieć. W tym podejściu informacje są gromadzone w postaci pakietów sieciowych, często przy użyciu urządzeń interfejsu sieciowego ustawionych w trybie przechwycenia. (Takie urządzenie działające w trybie promiscuous przechwytuje cały dostępny dla niego ruch sieciowy - zwykle w tym samym segmencie sieci - a nie tylko ruch adresowany do niego). Inne podejścia do wykonywania monitorowania sieciowego obejmują wykorzystanie portów łączących (wyspecjalizowane porty monitorowania, które umożliwiają przechwytywanie ruchu sieciowego ze wszystkich portów przełącznika) na przełącznikach sieciowych lub wyspecjalizowanych zaczepach sieci Ethernet (np. snifferach) w celu przechwytywania ruchu sieciowego.

Monitorowanie systemu operacyjnego.

Niektóre monitory zbierają dane ze źródeł wewnętrznych komputera. Różnią się one od monitoringu sieciowego poziomem abstrakcji, na którym gromadzone są dane. Monitorowanie oparte na hoście zbiera informacje z poziomu systemu operacyjnego (OS) komputera. Najczęstszymi źródłami danych na poziomie systemu operacyjnego są ścieżki audytu systemu operacyjnego, które są zwykle generowane w jądrze systemu operacyjnego, oraz dzienniki systemowe, które są generowane przez narzędzia systemu operacyjnego.

Monitorowanie aplikacji.

Monitorowanie oparte na aplikacjach zbiera informacje z uruchomionych aplikacji. Źródła informacji wykorzystywane w podejściach opartych na aplikacjach obejmują dzienniki zdarzeń aplikacji i informacje o konfiguracji aplikacji. Wraz ze wzrostem złożoności systemów stale rośnie znaczenie źródeł informacji opartych na aplikacjach. Pojawienie się technik programowania zorientowanego obiektowo wprowadza konwencje nazewnictwa obiektów danych, które niweczą większość zdolności analityka do zrozumienia dzienników dostępu do plików. W tej sytuacji poziom aplikacji jest jedynym miejscem w systemie, w którym można „zobaczyć" dostęp do danych na odpowiednim poziomie abstrakcji, który może ujawnić naruszenia bezpieczeństwa. Jeden szczególny przypadek monitorowania w oparciu o aplikacje obejmuje całą kategorię produktów w zakresie bezpieczeństwa. Ten typ systemu (czasami nazywany wykrywaniem wytłaczania) monitoruje transfery danych, szukając anomalii związanych z przemieszczaniem danych przez granice polityki. Takie monitorowanie danych jest bardzo popularne jako mechanizm zgodności dla przedsiębiorstw zajmujących się danymi konsumenckimi, finansowymi lub innymi danymi podlegającymi regulacjom.

Inne rodzaje monitorowania.

Jak wspomniano, źródła informacji o wykrywaniu włamań nie są ograniczone do nieprzetworzonych danych o zdarzeniach. W rzeczywistości, umożliwienie systemom wykrywania włamań działania na wynikach z innych systemów często optymalizuje jakość wyników systemu wykrywania włamań. Gdy dane są dostarczane przez inne części infrastruktury bezpieczeństwa systemu (np. Zapory sieciowe, programy do sprawdzania integralności plików, skanery antywirusowe lub inne systemy wykrywania włamań), czułość i niezawodność wyników systemu wykrywania włamań może znacznie wzrosnąć.

Problemy ze źródłami informacji.

Istnieje kilka problemów dotyczących źródeł informacji służących do wykrywania włamań. Najważniejsze z nich, które przetrwały w historii wykrywania włamań, to:

* W systemach opartych na hoście musi istnieć równowaga między zbieraniem wystarczającej ilości informacji, aby dokładnie przedstawić naruszenia bezpieczeństwa, a gromadzeniem tak dużej ilości informacji, że proces gromadzenia uszkodzi monitorowany system.

* Wierność procesu wykrywania włamań zależy nie tylko od zebrania odpowiednich informacji, ale także od zebrania ich z odpowiednich punktów obserwacyjnych w monitorowanym systemie lub sieci.

* Jeśli IDS ma tworzyć zapisy zdarzeń, które będą wykorzystywane do wspierania procesów prawnych, system musi zbierać i obsługiwać informacje o zdarzeniach w sposób zgodny z prawnymi zasadami dowodowymi.

* Informacje zbierane przez IDS często zawierają informacje o charakterze wrażliwym. Informacje te muszą być zabezpieczone i przetwarzane w sposób zgodny z normami prawnymi i etycznymi.

SCHEMATY ANALIZ

Po zdefiniowaniu i umieszczeniu źródeł informacji i czujników, zebrane w ten sposób informacje muszą zostać przeanalizowane pod kątem oznak ataku. Silnik analizy służy do wykrywania włamań, przyjmowania danych o zdarzeniach ze źródła informacji i badania ich pod kątem symptomów problemów z bezpieczeństwem. Jak wspomniano wcześniej, systemy wykrywania włamań zazwyczaj zapewniają funkcje analizy, które można podzielić na dwie kategorie: wykrywanie nadużyć i wykrywanie anomalii.

Wykrywanie niewłaściwego użycia.

Wykrywanie nadużyć to filtrowanie strumieni zdarzeń pod kątem wzorców aktywności, które odzwierciedlają znane ataki lub inne naruszenia zasad bezpieczeństwa. Detektory nadużyć używają różnych algorytmów dopasowywania wzorców, operując na dużych bazach danych wzorców lub sygnatur ataków. Większość obecnych komercyjnych systemów wykrywania włamań obsługuje wykrywanie nadużyć. Wykrywanie nadużyć zakłada, że istnieje jasne zrozumienie polityki bezpieczeństwa systemu, która może wyrażać się we wzorcach odpowiadających pożądanej i niepożądanej aktywności. Dlatego podpisy można opisać w kategoriach „to nigdy nie powinno się zdarzyć", a także „tylko to powinno się kiedykolwiek zdarzyć". Podpisy mogą również obejmować od uproszczonych kontroli atomowych (jednoczęściowych) do raczej złożonych kontroli złożonych (wieloczęściowych). Przykładem atomowego sprawdzenia jest sygnatura przepełnienia bufora, w której szuka się określonego polecenia, po którym następuje ciąg znaków przekraczający określoną długość. Przykładem sprawdzenia złożonego jest sygnatura stanu wyścigu, w której występuje seria starannie ustawionych w czasie poleceń. Podpisy są gromadzone i konstruowane w pewien sposób, aby zoptymalizować filtrowanie danych o zdarzeniach względem nich. Kolejnym wymogiem wykrywania nadużyć jest zakodowanie danych o zdarzeniach zebranych ze źródeł informacji w sposób umożliwiający ich porównanie z danymi podpisu. Można to zrobić na różne sposoby, od dopasowywania wyrażeń regularnych (czasami nazywanych dopasowywaniem „brudnych słów") po złożone schematy kodowania obejmujące diagramy stanów i kolorowe sieci Petriego. Diagramy stanu to schematy graficzne służące do modelowania włamań. Wyrażają intruzje w postaci stanów, reprezentowanych przez węzły lub okręgi, oraz przejść, reprezentowanych przez linie lub łuki. Kolorowe sieci Petriego są rozszerzeniem techniki diagramów stanów, które dodają kolorowe żetony, które zajmują węzły stanu i których kolor wyraża informacje o kontekście stanu. W niektórych IDS i IPS opartych na zawartości znaczące zasoby są przeznaczone na identyfikację sformatowanych pakietów sieciowych, zwłaszcza tych, w których format zawartości pakietu nie odpowiada formatowi usługi (np. SMTP) lub powiązanemu numerowi portu pakietu. Ten zniekształcony schemat pakietów stanowi

jedną z głównych kategorii ataków DDoS, które mają na celu odmowę dostępu do sieci legalnym użytkownikom.

Wykrywanie anomalii.

Wykrywanie anomalii to analiza strumieni zdarzeń systemowych, charakteryzująca je przy użyciu technik statystycznych i innych technik klasyfikacji w celu znalezienia wzorców aktywności, które wydają się odbiegać od normalnego działania systemu. Podejście to opiera się na założeniu, że ataki i inne naruszenia zasad bezpieczeństwa są podzbiorem nietypowych zdarzeń systemowych. Do wykrywania anomalii wykorzystuje się kilka popularnych technik:

* Analiza ilościowa. Większość nowoczesnych systemów wykorzystujących wykrywanie anomalii zapewnia analizę ilościową, w której reguły i atrybuty są wyrażane w postaci liczbowej. Najpowszechniejszymi formami analizy ilościowej są wyzwalacze i progi, w których atrybuty systemu są wyrażane jako zliczenia występujące w pewnym przedziale czasu, z pewnym poziomem określanym jako dopuszczalny. Wyzwalacze i progi mogą być proste, w których dopuszczalny poziom jest stały lub heurystyczny, w których dopuszczalny poziom jest dostosowywany do obserwowanych poziomów. Systemy zapobiegania włamaniom do sieci, których celem są ataki DDoS, często używają heurystycznych wyzwalaczy i progów do scharakteryzowania normalnego obciążenia przepustowości, szybkości połączeń i liczby połączeń w ruchu sieciowym.

* Analiza statystyczna. Większość systemów wczesnego wykrywania anomalii wykorzystywała techniki statystyczne do identyfikacji nieprawidłowych danych. W analizie statystycznej profile są budowane dla każdego użytkownika i zasobu systemowego, a statystyki są obliczane dla różnych atrybutów użytkownika i zasobów dla określonego przedziału czasu (zwykle jest to „sesja", definiowana jako czas, który upłynął od zalogowania do wylogowania).

* Techniki uczenia się. Odnotowano duże zainteresowanie badawcze wykorzystaniem różnych technik uczenia się, takich jak sieci neuronowe i logika rozmyta, do wykrywania anomalii. Pomimo zachęcających wyników, istnieje wiele praktycznych przeszkód w stosowaniu tych technik w środowiskach produkcyjnych. Praktyczne przeszkody powstają z powodu niedopasowania między atrybutami, które są odpowiednie do charakteryzowania przez sieci neuronowe i logikę rozmytą, a atrybutami, które są wykonywane przez personel operacyjny i systemy. Wartość korzystania z sieci neuronowych (większość z nich wykorzystuje logikę rozmytą) polega na tym, że potrafią one scharakteryzować i rozpoznać bardzo subtelne oznaki problemów w systemach. Ma to znaczenie w sytuacjach, w których wykrywane problemy nie są subtelne. Jednak w przypadku naruszeń bezpieczeństwa, na różnicę między normalnym zachowaniem a atakiem bezpieczeństwa często wpływa kontekst systemu; w tych scenariuszach niewiele, jeśli w ogóle, sieci neuronowe mogą dostarczyć wglądu w to, w jaki sposób podjęły decyzje dotyczące podejrzanych zdarzeń, które wyzwalają. Osoba odpowiedzialna za ochronę w kontekście operacyjnym zwykle potrzebuje tego rodzaju wglądu, aby opracować odpowiednią reakcję na wykryte włamanie.

* Zaawansowane techniki. Wykrywanie anomalii stosowane do wykrywania włamań pozostaje aktywnym obszarem badań. Ostatnie wysiłki badawcze obejmują zastosowanie tak zaawansowanych technik analitycznych, jak algorytmy genetyczne, eksploracja danych, czynniki autonomiczne i podejścia do układu odpornościowego, do problemu rozpoznawania nowych ataków i naruszeń bezpieczeństwa. Ponownie, techniki te nie były jeszcze szeroko rozpowszechnione w komercyjnych systemach IDS, chociaż pojawiły się w produktach specjalnego przeznaczenia

Podejścia hybrydowe.

Istnieją poważne problemy związane zarówno z wykrywaniem nadużyć, jak i metodami wykrywania anomalii w analizie zdarzeń w celu wykrywania włamań; jednakże połączenie obu podejść zapewnia znaczne korzyści. Silnik wykrywania anomalii może umożliwić IDS wykrywanie nowych lub nieznanych ataków lub naruszeń zasad. Jest to szczególnie cenne, gdy system docelowy chroniony przez IDS jest dobrze widoczny w Internecie lub innej sieci wysokiego ryzyka. W IPS wykrywanie anomalii zastosowane do atrybutów ruchu sieciowego jest jednym z jedynych sposobów radzenia sobie z atakami DDoS typu packet-flood, które są coraz większym problemem w dzisiejszych sieciach. Z kolei silnik wykrywania nadużyć chroni integralność niektórych silników wykrywania anomalii, zapewniając, że przeciwnik będący pacjentem nie może stopniowo zmieniać wzorców zachowań w czasie, aby ponownie wyszkolić detektor anomalii, aby akceptował zachowanie ataku w normalny sposób. znaczące niedociągnięcia w wykrywaniu anomalii ze względów bezpieczeństwa.

Zagadnienia w analizie.

Oto kilka z wielu problemów występujących w analizie wykrywania włamań:

* Systemy wykrywania nadużyć, chociaż bardzo skuteczne w wykrywaniu scenariuszy, dla których zdefiniowano sygnatury wykrywania, nie mogą wykrywać nowych ataków.

* Systemy wykrywania anomalii są w stanie wykryć nowe ataki, ale zwykle mają tak wysokie wskaźniki fałszywie pozytywnych odpowiedzi, że użytkownicy często ignorują generowane przez siebie alarmy.

* Systemy wykrywania anomalii, które opierają się na technikach sztucznej inteligencji (AI), często cierpią z powodu braku odpowiednich danych szkoleniowych. (Dane są używane do zdefiniowania logiki detektora w celu odróżnienia zdarzeń „normalnych” od „nienormalnych”).

* Złoczyńcy z uprawnieniami dostępu do systemu, podczas gdy systemy wykrywania anomalii są szkolone, mogą potajemnie uczyć system akceptowania określonych wzorców nieautoryzowanych działań w normalny sposób. Później systemy wykrywania anomalii zignorują faktyczne niewłaściwe użycie.

ODPOWIEDŹ.

Ostatni etap wykrywania włamań, reagowania, to działania podejmowane w odpowiedzi na naruszenia bezpieczeństwa wykryte przez IDS. Odpowiedzi są podzielone na opcje pasywne i aktywne. Różnica między odpowiedziami biernymi i aktywnymi polega na tym, czy za reakcję na wykryte naruszenia odpowiada użytkownik systemu IDS, czy też sam system. Jak już wspomniano, pierwsza opcja jest związana z klasycznym IDS; ta ostatnia jest związana z IPS.

Odpowiedzi pasywne.

Po wybraniu odpowiedzi pasywnych IDS po prostu dostarcza wyniki procesu wykrywania użytkownikowi, który musi następnie działać na tych wynikach, niezależnie od IDS. W tej opcji użytkownik ma pełną kontrolę nad reakcją na wykryty problem. W niektórych IDS informacje przekazywane użytkownikowi dotyczące wyników detekcji można podzielić na alarmy i raporty.

Alarmy.

Alarmy to komunikaty, które są natychmiast przekazywane użytkownikom. Komercyjne systemy wykrywania włamań wykorzystują różne kanały do przekazywania tych alarmów personelowi ochrony. Najczęściej jest to ekran wiadomości lub ikona zapisywana na konsoli sterowania IDS. Inne kanały alarmowe obejmują pagery, pocztę elektroniczną, komunikację bezprzewodową i pułapki systemu zarządzania siecią.

Raporty.

Raporty to wiadomości lub grupy wiadomości, które są generowane okresowo. Zazwyczaj dokumentują wydarzenia, które miały miejsce w przeszłości i często zawierają zagregowane dane liczbowe i informacje o trendach. Wiele komercyjnych produktów IDS obsługuje rozbudowane funkcje raportowania, umożliwiając użytkownikowi skonfigurowanie automatycznego generowania raportów w kilku wersjach, z których każda jest przeznaczona dla innego poziomu zarządzania.

Aktywne odpowiedzi: Man-in-the-Loop i autonomiczne.

Gdy IDS zapewnia aktywne opcje odpowiedzi, zwykle dzielą się one na dwie kategorie. Pierwsza wymaga od IDS podjęcia działań, ale przy aktywnym udziale interaktywnego użytkownika. Ta opcja jest czasami nazywana mechanizmem man-in-the-loop. Ta opcja jest preferowana w przypadku krytycznych systemów, ponieważ umożliwia operatorowi śledzenie napastnika lub interwencję w wrażliwej sytuacji w elastyczny i dokładny sposób. Druga opcja aktywnej odpowiedzi, która zwykle definiuje IPS, przewiduje wstępnie zaprogramowane działania podejmowane automatycznie przez system bez udziału człowieka. Opcja automatycznej odpowiedzi jest wymagana w przypadku niektórych rodzajów narzędzi do automatycznego ataku (wirusy lub robaki) lub ataków DDoS. Ataki te przebiegają z prędkością maszyny i dlatego znajdują się poza zasięgiem ręcznej interwencji kontrolowanej przez człowieka. Ponieważ ataki zautomatyzowane i ataki DDoS są najczęściej wybieranym narzędziem przez szantażystów online, liczba IPSów umieszczonych w sieciach komercyjnych gwałtownie wzrosła w ciągu ostatnich kilku lat.

Zautomatyzowane cele reakcji.

Odpowiedzi automatyczne obsługują trzy kategorie celów odpowiedzi:

1. Zbieranie dodatkowych informacji o wtargnięciu lub intruzie

2. Zmiana środowiska (np. Zmiana ustawień przełącznika lub routera w celu odmowy dostępu intruzowi)

3. Podejmowanie działań przeciwko intruzowi

Chociaż ostatnia z tych grup, czasami oznaczana jako kontratak lub hack back, czasami jest omawiana w kręgach bezpieczeństwa, inne opcje są znacznie bardziej produktywne w większości sytuacji. W tej chwili podjęcie działań przeciwko intruzowi jest uważane za niewłaściwe w prawie wszystkich sytuacjach i powinno być podejmowane wyłącznie za radą i radą organu prawnego. Zmiana otoczenia i gromadzenie większej ilości informacji może odbywać się w trybie samodzielnym lub zintegrowanym.

Samodzielne odpowiedzi.

Niektóre automatyczne odpowiedzi są zaprojektowane tak, aby wykorzystywać funkcje, które są całkowicie objęte systemem wykrywania włamań. Na przykład system wykrywania włamań może mieć specjalne reguły wykrywania, bardziej czułe lub szczegółowe niż te dostępne w normalnych trybach pracy. W samodzielnej odpowiedzi adaptacyjnej IDS użyłby bardziej wrażliwych reguł, gdy zostanie wykryty dowód preambuły ataku. Dzięki temu system IDS może zwiększać poziom czułości tylko wtedy, gdy potrzebne są dodatkowe możliwości wykrywania, co zmniejsza liczbę fałszywych alarmów.

Zintegrowane odpowiedzi.

Opcja odpowiedzi często uważana za najbardziej produktywną polega na użyciu zintegrowanych środków, które zmieniają ustawienia systemu, aby zablokować działania atakującego. Takie odpowiedzi mogą mieć wpływ na konfigurację systemu docelowego, hosta IDS / IPS lub sieci, w której

oba znajdują się. W pierwszym przypadku IDS / IPS może zmienić ustawienia mechanizmów logowania na hoście docelowym, aby zwiększyć ilość lub rodzaj gromadzonych informacji. IDS może również zmienić swój silnik analityczny, aby rozpoznawać bardziej subtelne oznaki ataku. W innej opcji odpowiedzi odzwierciedlonej w produktach komercyjnych system IDS odpowiada na zaobserwowaną sygnaturę ataku, wysyłając zapytanie do systemu docelowego w celu ustalenia, czy jest on podatny na ten konkretny atak. Jeśli luka jest obecna, IDS kieruje system docelowy do naprawy tej luki. W efekcie ten proces zapewnia system docelowy z funkcją odpornościową i pozwala mu się „leczyć", albo bezpośrednio blokując atak, albo też interaktywnie naprawiając wszelkie szkody wyrządzone w trakcie ataku. Wreszcie, niektóre systemy mogą wykorzystywać specjalne systemy wabików, zwane pojemnikami na miód lub wyścielanymi komórkami, jako odwrócenie uwagi napastników. Gdy te systemy są zapewnione, IDS może być skonfigurowany do przekierowywania napastników do środowisk wabików. W szczególnym przypadku zintegrowanej odpowiedzi, występującym w wielu komercyjnych ofertach IPS, IPS jest zintegrowany z przełącznikiem lub routerem. Po wykryciu ataku przełącznik lub router jest rekonfigurowany w locie, aby zablokować źródło ataku. Inne oferty IPS zaprojektowane do radzenia sobie z atakami DDoS wykorzystują wiele IDS / IPS do wykrywania ataków, a następnie manipulują strukturą przełączającą, aby przekierować ataki z docelowych systemów. Z biegiem czasu takie funkcje IPS zostaną prawdopodobnie zintegrowane z urządzeniami infrastruktury sieciowej, podobnie jak wiele funkcji zapory.

Wsparcie dochodzeniowe.

Chociaż głównym celem projektowania systemów wykrywania włamań jest wykrywanie ataków i innych potencjalnie problematycznych zdarzeń systemowych, informacje gromadzone i archiwizowane przez systemy wykrywania włamań mogą również wspierać osoby odpowiedzialne za badanie incydentów bezpieczeństwa. Ten wymóg funkcjonalny może nakładać dodatkowe wymagania techniczne na IDS. Na przykład, jeśli badacze planują wykorzystać funkcje monitorowania IDS do prowadzenia ukierunkowanego nadzoru nad trwającym atakiem, bardzo ważne jest, aby źródła informacji były „ciche", aby przeciwnicy nie byli świadomi, że są monitorowani. Ponadto osoby monitorujące IDS muszą być w stanie przekazywać informacje śledczym zaufanym, bezpiecznym kanałem. Wreszcie, sam system IDS musi znajdować się pod kontrolą śledczych lub innych zaufanych stron; w przeciwnym razie przeciwnicy mogą maskować swoje działania, wybiórczo podszywając się pod źródła informacji. Być może najważniejszą rzeczą, o której badacze powinni pamiętać o IDS, jest to, że dostarczone informacje powinny być potwierdzone przez inne źródła informacji (np. Dzienniki urządzeń infrastruktury sieciowej), niekoniecznie akceptowane według wartości nominalnej.

Problemy w odpowiedziach.

Podobnie jak w przypadku źródeł informacji i strategii analitycznych, pewne problemy związane z funkcjami reagowania IDS przetrwały w historii wykrywania włamań. Główne kwestie to:

* Potrzeby użytkowników w zakresie możliwości reagowania IDS są tak różne, jak sami użytkownicy. W niektórych środowiskach systemowych komunikaty odpowiedzi systemu IDS są monitorowane przez całą dobę, a administratorzy systemu podejmują działania w czasie rzeczywistym na podstawie alarmów IDS. W innych środowiskach użytkownicy mogą używać odpowiedzi systemu wykrywania włamań w postaci raportów jako miernika wskazującego środowisko zagrożenia, w którym znajduje się określony system. Przy wyborze IDS należy wziąć pod uwagę specyficzne potrzeby użytkownika

* Biorąc pod uwagę fałszywie dodatnie poziomy błędów dla IDS, opcje odpowiedzi muszą być dostrajane przez użytkowników. W przeciwnym razie użytkownicy po prostu wyłączą odpowiedzi IDS. To unieważnia wartość IDS.

* Gdy IDS zapewnia automatyczne odpowiedzi na wykryte problemy, istnieje ryzyko, że IDS sam przeprowadzi skuteczny atak typu „odmowa usługi" na chroniony przez siebie system. Załóżmy na przykład, że IDS jest skonfigurowany z regułami, które mówią mu „po wykryciu ataku z danego adresu IP skieruj zaporę ogniową tak, aby blokowała późniejszy dostęp z tego adresu IP". Atakujący, wiedząc, że system IDS jest tak skonfigurowany, może przeprowadzić atak za pomocą sfałszowanego adresu źródłowego IP, który wydaje się pochodzić od głównego klienta lub partnera organizacji. IDS rozpozna atak, a następnie zablokuje dostęp tej organizacji na pewien czas, powodując odmowę usługi.

OCENA POTRZEB I WYBÓR PRODUKTU.

Wartość produktów do wykrywania włamań w ramach strategii bezpieczeństwa organizacji jest optymalizowana poprzez dokładną ocenę potrzeb. Te potrzeby i cele związane z bezpieczeństwem mogą służyć jako wskazówki przy wyborze produktów, które poprawią stan bezpieczeństwa organizacji.

Dopasowanie potrzeb do funkcji.

Potrzeby, na które najczęściej odpowiadają systemy wykrywania i zapobiegania włamaniom, obejmują:

* Zapobieganie problematycznym zachowaniom poprzez zwiększenie ryzyka wykrycia i ukarania atakujących systemu.

* Wykrywanie naruszeń bezpieczeństwa, którym nie zapobiegły (lub nawet w niektórych przypadkach nie można było zapobiec) za pomocą innych środków bezpieczeństwa.

* Dokumentacja istniejącego poziomu zagrożenia dla systemów komputerowych i sieci organizacji.

* Wykrywanie i, jeśli to możliwe, łagodzenie preambuł ataku. (Obejmuje to takie działania, jak sondy sieciowe, skanowanie portów i inne tego typu „brzęczenie klamkami").

* Diagnoza problemów w innych elementach infrastruktury bezpieczeństwa (tj. Awarie czy błędne konfiguracje).

* Zapewnienie personelowi odpowiedzialnemu za bezpieczeństwo systemu możliwości testowania efektów bezpieczeństwa działań konserwacyjnych i modernizacyjnych w sieciach organizacyjnych.

* Dostarczanie informacji o naruszeniach, które mają miejsce, umożliwiając śledczym ustalenie i usunięcie pierwotnych przyczyn.

* Dostarczenie dowodów zgodności z danym wymogiem prawnym dotyczącym ochrony informacji. Stanowi to istotną potrzebę dla członków różnych regulowanych branż, takich jak bankowość i opieka zdrowotna.

Bez względu na to, które z tych konkretnych potrzeb są istotne dla użytkownika, ważne jest, aby rozważyć zdolność systemu wykrywania włamań do zaspokojenia potrzeb określonego środowiska, w którym jest zainstalowany. Krytyczną częścią tego określenia jest rozważenie, czy system wykrywania włamań ma możliwość monitorowania określonych źródeł informacji dostępnych w środowisku docelowym. Jeszcze ważniejsze jest to, czy polityka bezpieczeństwa organizacji przekłada się na politykę monitorowania i wykrywania, którą można wykorzystać do skonfigurowania IDS (lub w przypadku IPS, politykę monitorowania, wykrywania i reagowania). Struktura zabezpieczeń polityka ma szczególne znaczenie dla powodzenia IPS.

Scenariusze szczególne.

Nie ma powszechnie stosowanego opisu sieci komputerowych lub systemów IDS, które je chronią. Istnieją jednak pewne typowe scenariusze, biorąc pod uwagę aktualne trendy w korzystaniu z sieci i systemu. Popularnym uzasadnieniem stosowania IDS na wczesnym etapie cyklu życia bezpieczeństwa organizacji jest ustalenie poziomu zagrożenia dla danej enklawy sieciowej. W tym celu często wykorzystuje się sieciowe systemy IDS, z monitorami umieszczonymi poza zaporą organizacyjną. Ci, którzy są odpowiedzialni za zdobycie wsparcia zarządzania dla wysiłków związanych z bezpieczeństwem, często uważają to użycie IDS za bardzo pomocne. Wiele organizacji używa IDS do ochrony serwerów WWW. W takim przypadku charakter interakcji między serwerem WWW a użytkownikami wpłynie na wybór i konfigurację IDS. Większość serwerów Web pełni dwa rodzaje funkcji: (1) informacyjne (np. Serwery WWW obsługujące proste zapytania HTTP i FTP od użytkowników) i (2) transakcyjne (np. Serwery WWW, które umożliwiają interakcję użytkownika wykraczającą poza zwykły ruch HTTP lub FTP). Transakcyjne serwery WWW są zwykle trudniejsze do monitorowania niż serwery informacyjne, ponieważ zakres interakcji między użytkownikami a serwerami jest szerszy. W przypadku krytycznych transakcyjnych serwerów WWW kierownicy ds. Bezpieczeństwa mogą chcieć rozważyć wiele IDS, monitorując serwery na wielu poziomach abstrakcji (tj. Aplikacji, hosta i sieci). Trzeci scenariusz obejmuje organizacje, które chcą używać IDS jako dodatkowej ochrony określonych części swoich systemów sieciowych. Przykładem tego jest organizacja medyczna, która chce chronić systemy baz danych pacjentów przed naruszeniami prywatności. W tej sytuacji, jak w podanym właśnie przykładzie serwera WWW, może być wskazane użycie wielu IDS, monitorujących interakcje na wielu poziomach abstrakcji. Dane wyjściowe tych wielu systemów można zsynchronizować, a niespójności można zauważyć w celu wiarygodnego wskazania poziomów zagrożenia. Innym przykładem, który jest coraz bardziej powszechny, jest organizacja, która troszczy się o łączność bezprzewodową. W tym przypadku monitoringu WiFi produkty są dostępne na rynku, z funkcjami gromadzenia informacji i monitorowania podobnymi do tych, które mają klasyczne systemy IDS. W ostatnich latach coraz szersze wykorzystanie bezprzewodowych sieci lokalnych (WLAN) w budynkach i kampusach stymulowało rozwój bezprzewodowych systemów wykrywania i zapobiegania włamaniom (WIDPS). Podstawowe zasady są takie same, jak w przypadku innych systemów IDS i IPS, z dodatkiem jednej interesującej pomyłki: WIDPS są często używane do wykrywania nieautoryzowanych punktów dostępu zainstalowanych w sieciach WLAN organizacji przez nieuczciwych pracowników lub intruzów. Karen Scarfone i Peter Mell w wydaniu NIST SP 800-94 z lipca 2012 r. Zwracają uwagę, że czujniki WIDPS należy umieszczać w obszarach, w których nie powinno być żadnej aktywności sieci bezprzewodowej. Niektórzy menedżerowie bezpieczeństwa przechodzą i omijają swoje obiekty z narzędziami WIDPS na swoich laptopach w celu identyfikacji nieautoryzowanych punktów dostępu. Nie można jednak wykryć całkowicie pasywnego podsłuchiwania ruchu w sieci WLAN. W rozległych sieciach, jeśli architekt bezpieczeństwa zdecyduje się na nałożenie wielu systemów IDS i IPS na warstwy, może być wymagany monitor zdarzeń bezpieczeństwa / menedżer informacji o bezpieczeństwie (SIM / SEM). Taki system byłby niezbędny do skonsolidowania i zintegrowania wyników każdego IDS / IPS w spójny zestaw wniosków.

Integracja produktów IDS z infrastrukturą bezpieczeństwa.

Jak wspomniano, IDS nie zastępuje zapory, wirtualnej sieci prywatnej, pakietu do identyfikacji i uwierzytelniania ani żadnego innego produktu punktu bezpieczeństwa. Jednak system IDS może poprawić jakość ochrony zapewnianej przez inne produkty punktowe, monitorując ich działanie, odnotowując oznaki nieprawidłowego działania lub obejścia. Ponadto IPS może współdziałać z pozostałymi produktami punktowymi, aby pomóc zablokować trwający atak.

Wdrażanie produktów IDS.

Pierwsze generacje instalacji IDS dostarczyły pewnych spostrzeżeń związanych z wdrażaniem IDS. Kluczowe punkty to lokalizacja czujników, planowanie integracji IDS, dostosowywanie ustawień alarmów i outsourcing usług IDS / IPS.

Lokalizacja czujników.

Istnieją cztery ogólne lokalizacje czujników IDS:

1. Poza główną zaporą organizacyjną

2. W sieci DMZ (wewnątrz głównej zapory, ale poza wewnętrznymi zaporami)

3. Za wewnętrznymi zaporami ogniowymi

4. W krytycznych podsieciach, w których znajdują się krytyczne systemy i dane

Jak wspomniano, czujniki IDS umieszczone poza główną zaporą organizacyjną są przydatne do określenia poziomu zagrożenia dla danej sieci. Czujniki umieszczone w DMZ13 mogą monitorować próby penetracji serwerów internetowych. Monitory IDS do użytku wewnętrznego ataku są przeprowadzane na wewnętrzne segmenty sieci, za wewnętrznymi zaporami ogniowymi. W przypadku krytycznych podsieci czujniki IDS są zwykle umieszczane w przepustach, w których podsieci są połączone z resztą sieci firmowej. W przypadku sieci bezprzewodowych wyspecjalizowane urządzenia IPS służą do wykrywania i zgłaszania nieautoryzowanego dostępu do sieci za pośrednictwem punktów dostępu WLAN lub punktów dostępu otwartego oprogramowania, poprzez źle skonfigurowane interfejsy WLAN w laptopach i innych urządzeniach WLAN. Te urządzenia IPS są zwykle umieszczane za zaporami i rozmieszczone w przestrzeni fizycznej zajmowanej przez organizację i jej użytkowników.

Harmonogram integracji IDS.

Wczesne generacje produktów do wykrywania włamań udowodniły, że nie wolno przyspieszać procesów integracji. Systemy IDS nadal polegają na interakcjach operatora w celu eliminowania fałszywych alarmów i reagowania na uzasadnione alarmy. W związku z tym niezwykle ważne jest, aby procesy zapewniały personelowi operacyjnemu odpowiednią ilość czasu na poznanie zachowania IDS w systemach docelowych, rozwijając poczucie, w jaki sposób IDS współpracuje z poszczególnymi komponentami systemu w różnych sytuacjach. Ta mądrość odnosi się jeszcze bardziej do instalacji IPS, gdzie błąd w określeniu odpowiedzi może mieć katastrofalne skutki dla funkcjonowania sieci o znaczeniu krytycznym.

Ustawienia alarmu.

Systemy IDS charakteryzują się znacznymi wskaźnikami fałszywych alarmów, w niektórych sytuacjach nawet 80 procent. Wielu doświadczonych integratorów IDS zaleca zawieszenie alarmów na okres tygodni, nawet miesiące, gdy operatorzy zapoznają się z systemem IDS i systemami docelowymi. Szczególnie rozsądne jest opóźnienie aktywacji automatycznych odpowiedzi na ataki, dopóki operatorzy i administratorzy systemu nie zapoznają się z IDS i nie dostosują go do środowiska docelowego.

Outsourcing IDS / IPS.

Wszelkie dyskusje na temat strategii IDS i IPS byłyby niepełne bez wzmianki o outsourcingu tych usług bezpieczeństwa. Z takim podejściem wiążą się znaczące korzyści, zwłaszcza w przedsiębiorstwach zbyt małych, aby pozwolić sobie na rozbudowany personel ochrony. Podobnie jak w innych obszarach outsourcingu IT, aby podejście to było skuteczne, trzeba mieć niezwykle jasne wyobrażenie o konkretnych pożądanych celach bezpieczeństwa i operacyjnych. Niezbędna jest jasno sformułowana

polityka bezpieczeństwa, która odzwierciedla aktualne obawy. Zalet outsourcingu jest wiele: dostawcy zarządzanych usług ochrony zwykle mają duże doświadczenie w pracy ze sprzętem IDS i IPS, ich pracownicy są często dobrze wyszkoleni i doświadczeni w obsłudze sprzętu, personel monitorujący jest zwykle obecny przez całą dobę, oraz warunki umowy często obejmują określone poziomy umów serwisowych. Mówiąc słowami mądrego CISO, „outsourcing to nie odciążanie". Oznacza to, że outsourcing funkcji bezpieczeństwa nie zwalnia Cię z odpowiedzialności za bezpieczeństwo systemu. Oznacza to również, że musisz zachować należytą staranność przy wyborze dostawcy usług, przydzielaniu mu zadań i zarządzaniu nim oraz monitorowaniu, aby zapewnić, że Twoje cele polityki są dobrze obsługiwane przez dostawcę.

WNIOSEK

Wykrywanie włamań i zapobieganie włamaniom to cenne dodatki do pakietów bezpieczeństwa systemu, umożliwiające kierownikom ds. Bezpieczeństwa wykrywanie, a czasami blokowanie naruszeń bezpieczeństwa, które nieuchronnie występują pomimo zastosowania prewencyjnych środków bezpieczeństwa. Chociaż obecne produkty komercyjne są niedoskonałe, służą do rozpoznawania wielu typowych typów włamań, w wielu przypadkach wystarczająco szybko, aby umożliwić personelowi ochrony i systemom IPS blokowanie uszkodzeń systemów i danych. Ponadto wraz z postępem prac badawczo-rozwojowych w zakresie wykrywania i zapobiegania włamaniom jakość i możliwości dostępnych systemów IDS i IPS będą stale się poprawiać.