Urządzenie Zabezpieczające Bramę

WPROWADZENIE

Zapora ogniowa, uznawana za wystarczającą do ochrony całej organizacji przed zagrożeniami zewnętrznymi, jest nadal prawdopodobnie najbardziej rozpoznawalnym i wdrażanym urządzeniem zabezpieczającym sieć do operacji związanych z Internetem. Jednak wcześniejsze generacje zapór ogniowych podejmowały decyzje dotyczące bezpieczeństwa przy niewielkim wsparciu kontekstowym innym niż pochodzenie i miejsce docelowe pakietów przechodzących przez określoną dozwoloną ścieżkę. Wraz ze wzrostem możliwości komunikacyjnych i wymagań w zakresie funkcjonalności wzrosła również potrzeba inspekcji i egzekwowania dozwolonych ścieżek przy użyciu bardziej złożonych protokołów i wymagającej coraz większej przepustowości. Ta ewolucja przekształciła zaporę ogniową w prawdziwe urządzenie zabezpieczające bramę (GSD) - zdolne do egzekwowania dozwolonych ścieżek przy użyciu kombinacji technik, które kiedyś wymagały dodatkowych urządzeń zabezpieczających. Właściwie dobrane i wdrożone GSD to jedna warstwa bezpieczeństwa zaprojektowana do obsługi tych coraz bardziej złożonych scenariuszy. GSD jest skuteczny tylko przy pełnym zrozumieniu możliwości i ograniczeń - zarówno operacyjnych, jak i awaryjnych - konsolidacji wielu funkcji bezpieczeństwa w jednym urządzeniu. Zapewniając egzekwowanie dozwolonych ścieżek w bardziej inteligentny i dokładny sposób, w połączeniu z dodatkowym rygorem prawdziwego zrozumienia oczekiwanych przepływów w sieci, GSD zapewniają wystarczającą dodatkową, głęboką ochronę w całej organizacji. Chociaż ten rozdział koncentruje się na GSD jako połączonym urządzeniu zabezpieczającym, omówione pojęcia są przydatne do zrozumienia i oceny funkcjonalności poszczególnych urządzeń zabezpieczających sieć. Każda organizacja musi podejmować decyzje dotyczące ryzyka i wyników, porównując to podejście z utrzymywaniem niezależnych urządzeń, które koncentrują się na określonej funkcji bezpieczeństwa.

Wymagania biznesowe przewyższające bezpieczeństwo.

Postęp technologiczny nieustannie zmienia zdolność przedsiębiorstwa do zarządzania cyklem życia danych. Wszechobecność urządzeń mobilnych i przechodzenie w kierunku zasobów przetwarzania w chmurze, które nie są już wyłącznie kontrolowane lub konsumowane przez organizację, wciąż na nowo definiuje granice. Użytkownicy coraz częściej żądają nieograniczonego dostępu do danych firmowych z dowolnego miejsca na dowolnym urządzeniu (w tym nie kontrolowanym przez organizację). To dynamiczne środowisko zwiększa potrzebę warstwowych architektur bezpieczeństwa z głębszą świadomością treści i kontekstu.

Przetwarzanie na żądanie

Przedsiębiorstwa, które nie posiadają niezbędnej wewnętrznej wiedzy kadrowej lub technologicznej niezbędnej do osiągnięcia celów organizacji w zakresie technologii informatycznych (IT), od dawna poszukują rozwiązań outsourcingowych, które spełnią ich potrzeby. Oprogramowanie jako usługa (SaaS) zapewnia takie oferty, jak aplikacje biurowe, współpraca i poczta e-mail (np. Microsoft Office365) oraz zarządzanie relacjami z klientami (CRM) (np. Salesforce.com). Infrastruktura i platforma jako usługa (odpowiednio IAAS i PAAS) zapewniają przechowywanie i przetwarzanie na żądanie (np. Amazon Web Services - S3 / EC2 lub Rackspace Open Cloud). Oferty zlecane na zewnątrz nadal dojrzewają i redefiniują sposób, w jaki przedsiębiorstwa rozwijają się, zarządzają i prezentują swoje informacje. Technologia wirtualizacji nadal zapewnia możliwości bardziej efektywnego wykorzystania wewnętrznych możliwości przetwarzania. Chociaż zapewnia lepszą wydajność, może również obniżyć poziom bezpieczeństwa, ponieważ istniejące oferty niekoniecznie są tak dojrzałe, jak dedykowana infrastruktura zabezpieczeń. Gdy systemy wewnętrzne i połączone z Internetem muszą działać w tej samej architekturze wirtualnej, stwarza to dodatkowe ryzyko, ponieważ systemy

współdziałają teraz na poziomie hiperwizora i przełącznika wirtualnego (vSwitch), na którym tradycyjne urządzenia zabezpieczające sieć nie są w stanie sprawdzić i wymusić ruchu na tym poziomie.

Wszechobecna mobilność.

Dzisiejszy klimat biznesowy wymaga od pracowników możliwości pracy z dowolnego miejsca, a ta potrzeba mobilności i elastyczności prowadzi do znaczącej zmiany w sposobie, w jaki organizacje definiują i chronią swoje granice. Pracownicy mogą korzystać z różnych systemów zarówno w pracy, w domu, jak iw podróży. Wymagany poziom dostępu i funkcjonalności wykracza daleko poza pocztę e-mail i obejmuje aplikacje i dane przedsiębiorstwa. Ponieważ mobilność funkcjonalna rozciąga się od urządzeń należących do firmy po urządzenia osobiste, organizacje muszą mieć metodę zapewniającą, że zagrożone urządzenie mobilne nie osłabi istniejących wewnętrznych lub zleconych na zewnątrz mechanizmów kontroli bezpieczeństwa.

Regulatory

Zgodność z przepisami i branżą.

Federalne wymagania regulacyjne nadal mają znaczący wpływ na sposób zarządzania ryzykiem przez organizacje poprzez działania w zakresie ochrony, przechowywania i prywatności danych - wiele z nich ma istotne wymagania dotyczące audytu i sprawozdawczości.

* Ustawa Sarbanes-Oxley (SOX) koncentruje się na kontrolach i procedurach mających na celu zachowanie integralności sprawozdawczości finansowej organizacji notowanych na giełdzie.

* Ustawa Gramm-Leach-Bliley Act (GLBA) - specyficzna dla instytucji finansowych - koncentruje się na ochronie danych klientów i prywatności.

* Ustawa o przenoszeniu i rozliczalności informacji zdrowotnych (HIPAA) wymaga ochrony danych umożliwiających identyfikację indywidualną, takich jak dane osobowe (PII) i chronione informacje zdrowotne (PHI).

Wymagania branżowe nadal pojawiają się i ewoluują, starając się sprostać minimalnym wymaganiom bezpieczeństwa niezbędnym do pracy z lub w ramach określonej branży. Standard Payment Card Industry Data Security Standard (PCI DSS) określa podstawowe wymagania dotyczące ochrony danych posiadaczy kart podczas przetwarzania, transmisji i przechowywania. PCI DSS wymaga od organizacji określenia ich poziomu zaangażowania w dane posiadaczy kart. Po ustaleniu określa, które wymagania są niezbędne do wykazania zgodności z normą. Każdy sektor infrastruktury krytycznej - zgodnie z definicją w Stanach Zjednoczonych przez Departament Bezpieczeństwa Wewnętrznego - ma plan sektorowy (SSP), który zapewnia reprezentatywnym organizacjom i agencjom narzędzia i strategie zarządzania ryzykiem specyficzne dla ochrony każdej branży. Jednym z bardziej dojrzałych programów jest North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP). NERC CIP zajmuje się wieloma fizycznymi i cyfrowymi elementami bezpieczeństwa północnoamerykańskiego systemu elektroenergetycznego, w tym ochroną bram poprzez ustanowienie elektronicznego obwodu bezpieczeństwa.

PODSTAWOWE POJĘCIA I TERMINOLOGIA.

Większe zapotrzebowanie na mobilność, nowe modele interakcji biznesowych i wykorzystanie możliwości przetwarzania w Internecie nadal wymuszają ewolucję tradycyjnych zabezpieczeń obwodowych.

Ogólne możliwości.

Przy znacznych wymaganiach przetwarzania wyspecjalizowanych systemów bezpieczeństwa sieci (np. IPS lub antyspam), organizacje tradycyjnie tworzyły infrastruktury bezpieczeństwa, które wykorzystywały dedykowane rozwiązania / urządzenia dla każdej funkcji. Jednak możliwości przetwarzania GSD obecnej generacji dają możliwość połączenia wielu z tych niegdyś dedykowanych systemów w jedno urządzenie.

Zunifikowane zarządzanie zagrożeniami.

Zunifikowane zarządzanie zagrożeniami (UTM) łączy elementy, takie jak ochrona przed złośliwym oprogramowaniem, antyspam, IDS / IPS, VPN, proxy aplikacji i filtrowanie treści - przekształcając zaporę ogniową w oryginalną iterację GSD. Te dodatkowe możliwości pozwalają UTM zapewnić lepszą kontrolę i inspekcję w warstwie aplikacji. Jednak zazwyczaj występowało tylko marginalne zarządzanie i integracja wydajności między zestawami funkcji.

Zapora nowej generacji.

Zapora nowej generacji (NGFW) to najnowsza ewolucja podanych możliwości, która uzupełnia i przewyższa te z UTM. Zamiast po prostu łączyć wiele technologii bezpieczeństwa jedna na drugą, NGFW zapewnia ściślejszą integrację każdego poziomu bezpieczeństwa. Te nowe możliwości obejmują większą świadomość protokołu i bardziej szczegółowe egzekwowanie dozwolonych ścieżek. NGFW jest w stanie profilować protokoły niezależnie od wybranego portu. Zwiększa to zdolność do wykrywania nieuczciwych zachowań, takich jak zaszyfrowane ładunki za pośrednictwem protokołów, które normalnie nie używają szyfrowania. Ta generacja GSD ma również możliwość dynamicznego dostosowywania polityki, rozszerzając ochronę na inne części infrastruktury bezpieczeństwa.

Zapory aplikacji sieci Web.

GSD zapewniają dodatkowe możliwości inspekcji i egzekwowania dozwolonych ścieżek dla komunikacji opartej na sieci Web. Jednak złożoność obecnych i następnej generacji protokołów internetowych może przewyższyć zabezpieczenia zapewniane przez to urządzenie. Zapora aplikacji sieci Web (WAF) zapewnia bardziej niezawodne możliwości inspekcji protokołu HTTP. WAF zapewnia konfigurowalne reguły w celu ochrony przed typowymi atakami opartymi na ładunku, takimi jak wstrzykiwanie SQL, XSS (skrypty między lokacjami) i wstrzykiwanie poleceń. Platforma ta może również służyć jako wirtualna łatka do aplikacji internetowych - starsza (bez możliwych poprawek) lub oczekująca na niepublikowane poprawki

Zmiana architektury zapory.

Ponieważ dostawcy zabezpieczeń starają się dotrzymać kroku tym zmianom, oferując większą funkcjonalność i wyższą wydajność, obowiązkiem klienta jest zrozumienie zalet i wad każdego proponowanego rozwiązania ochronnego. Taka analiza zapewnia organizacji niezbędny wgląd do wdrożenia najbardziej odpowiedniej architektury, aby spełnić niezbędne wymagania dotyczące bezpieczeństwa i wydajności

Filtrowanie pakietów.

Urządzenia rutujące dały początek możliwościom zapory ogniowej pierwszej generacji. Filtrowanie pakietów to zestaw jawnych reguł opisujących dozwolone ścieżki, którymi może podróżować ruch sieciowy. Reguły w postaci listy kontroli dostępu (ACL) niezależnie oceniają jedną lub więcej części nagłówka każdego pakietu, aby podjąć decyzję o dozwolonej ścieżce. Filtr pakietów działa na każdym pakiecie jako indywidualna jednostka bez względu na pakiety, które przychodzą przed lub po. Chociaż ta metoda zapewnia bezpieczeństwo z najmniejszym narzutem niż inne architektury zapór, jest

podatna na kilka ataków na sieć i warstwę transportową. Fałszowanie protokołu internetowego (IP) to specjalnie spreparowanie pakietu w celu oszukania routera do przyjmowania ruchu, który wydaje się legalny. Atakujący skonfiguruje pakiet tak, aby wyglądał tak, jakby pochodził z sieci wewnętrznej, nawet jeśli przechodzi do interfejsu zewnętrznego. Atak typu Land wysyła sfałszowany pakiet TCP SYN do hosta, którego adres IP źródłowy i docelowy oraz port są równe, co może spowodować atak typu „odmowa usługi" na podatnym stosie sieciowym. Atak Teardrop celowo dzieli pakiet na fragmenty i manipuluje przesunięciem fragmentu, w którym przesunięcie poprzedniego fragmentu pokrywa się z przesunięciem następnego fragmentu. Gdy system odbierający ponownie złoży nakładające się fragmenty, stos sieciowy ulegnie awarii, powodując odmowę usługi. Chociaż zarówno ataki typu Land, jak i Teardrop wymagają wrażliwego urządzenia końcowego, początkowe filtry pakietów nie miały kontekstowego zrozumienia, aby powstrzymać takie ataki. Łagodzenie ataku Teardrop obejmuje implementację ponownego składania pakietów - ponowne łączenie fragmentów do oryginalnego pakietu, aby upewnić się, że ponownie połączony pakiet nie narusza podstawowych specyfikacji pakietu IP - przed przekazaniem do następnego przeskoku. Obecne generacje GSD używają inspekcji stanowej (omówionej w następnej kolejności) w celu przezwyciężenia wielu ograniczeń filtrowania pakietów. Jednak wiele urządzeń niezwiązanych z zabezpieczeniami używa filtrów pakietów w celu zapewnienia podstawowej ochrony swoich interfejsów administracyjnych i funkcji monitorowania.

Państwowa inspekcja.

Inspekcja państwowa identyfikuje i śledzi dodatkowe parametry w każdym pakiecie, dodając kontekst, reprezentując przepływy wzdłuż dozwolonych ścieżek jako połączenia sieciowe zamiast pojedynczych pakietów. Mimo że protokół IP i protokół datagramów użytkownika (UDP) są protokołami bezpołączeniowymi, zapora tworzy wirtualne połączenie, aby emulować swoje zorientowane połączeniowo odpowiedniki. Chociaż określone parametry śledzone w tabeli stanów różnią się u różnych dostawców GSD, tabela ta znajduje się w pamięci, co zapewnia bardziej wydajne przetwarzanie. Ponieważ filtr pakietów sprawdza pakiety indywidualnie, nie wpływa na zapory w architekturze z równoważeniem obciążenia lub przełączaniem awaryjnym. Jednak aby zapewnić trwałe połączenia w architekturach o wysokiej dostępności, inspekcja stanowa musi ustanowić i utrzymywać zsynchronizowaną kopię tabeli stanu w każdym z jej elementów wysokiej dostępności. Chociaż niektórzy dostawcy nadal utrzymują, że bezpośrednie połączenie szeregowe jest najbardziej niezawodną metodą połączenia, jest mało prawdopodobne, aby rozwiązania o wysokiej dostępności znajdowały się w fizycznej bliskości niezbędnej do połączenia szeregowego i zazwyczaj wykorzystują istniejące połączenia sieciowe do utrzymania synchronizacji stanu.

Brama warstwy aplikacji.

W miarę jak zagrożenia stawały się coraz bardziej wyrafinowane w istniejących dozwolonych ścieżkach, zapory dodały ochronę bramy warstwy aplikacji (ALG). Każdy serwer proxy specyficzny dla aplikacji (np. HTTP, RPC, FTP itp.) Działa jako dozwolony broker ścieżki dla połączenia, tworząc oddzielne połączenie zaplecza z innym hostem. Chociaż pełne połączenie to w rzeczywistości dwie niezależne sesje, ta dwoistość jest niewidoczna dla żądającego i serwera. Bycie połączeniem obsługiwanym przez brokera dodaje dodatkową warstwę ochrony poprzez ponowne zapisywanie potencjalnie zniekształconych żądań, weryfikację / wymuszanie zgodności z protokołem i uniemożliwienie bezpośredniej komunikacji między klientem a serwerem. Szczegółowa analiza ładunku zwiększa ilość czasu, jaką zapora poświęca na ocenę każdego pakietu, potencjalnie zmniejszając przepustowość dla innego ruchu sieciowego i zwiększając zapotrzebowanie na wystarczające zasoby przetwarzania. ALG może również powodować problemy, takie jak słaba wydajność protokołów wymagających minimalnego narzutu, a także nieoczekiwane problemy ze zgodnością wynikające z implementacji protokołów specyficznych dla dostawcy. Aktywny przegląd i zarządzanie pomogą zminimalizować wpływ ALG na operacje

Obecne urządzenia zabezpieczające bramy.

Firewall ewoluował ponownie, gdy ataki stawały się coraz bardziej złożone i skalowane. Stanowe filtrowanie i funkcjonalność bramy warstwy aplikacji skutecznie chronią przed określonymi znanymi wektorami ataków. Jednak wyrafinowanie ataków nowszej generacji szybko ujawniło, że te dwie funkcje nie były w stanie zapewnić niezbędnego poziomu ochrony. Dodatkowe możliwości zintegrowane z firewallem dały początek GSD. Początkowa iteracja GSD jest znana jako ujednolicone zarządzanie zagrożeniami (UTM). UTM to konsolidacja zapory ogniowej z wieloma dodatkowymi platformami bezpieczeństwa (np. Systemy zapobiegania włamaniom do sieci, filtr treści, ochrona przed spamem itp.) W jednym urządzeniu. Dostawcy UTM, którzy mieli silną obecność tylko w jednym lub dwóch środkach ochrony, musieli albo zintegrować produkt zabezpieczający innej firmy, albo stworzyć własną ofertę, aby wypełnić pełny pakiet zabezpieczeń. Była to również okazja do skonsolidowania możliwości zarządzania i monitorowania w celu stworzenia ujednoliconej platformy. Jednak UTM okazałby się nieco nieefektywny, ponieważ każdy pakiet jest przesyłany szeregowo przez różne silniki bezpieczeństwa, poważnie wpływając na wydajność w miarę wzrostu liczby włączonych zabezpieczeń. Najnowsza generacja GSD, znana jako zapory ogniowe nowej generacji (NGFW), zapewnia lepsze wykrywanie aplikacji, świadomość i egzekwowanie, a także ściślejszą integrację wszystkich warstw zabezpieczeń. Samo zwiększenie możliwości przetwarzania i kontroli nie wystarczyło, aby sprostać wymaganiom protokołów aplikacji obecnej generacji. Te protokoły są bardziej złożone pod względem formy i funkcji, mimo że mogą być zgodne z tradycyjną dozwoloną ścieżką, taką jak HTTP. NGFW musi również być w stanie dekodować i rozumieć wewnętrzne działanie aplikacji niezależnie od portu i wymuszać na wszystkich lub podzestawach protokołu. NGFW przetwarzają pakiety równolegle przez wybrane silniki bezpieczeństwa, aby zwiększyć wydajność i skoncentrować ochronę na określonym typie wykrytego ruchu.

Kontekst środowiska hosta.

Chociaż skupiamy się na urządzeniach zabezpieczających bramy z punktu widzenia sieci, porównywalne zabezpieczenia oparte na hostach gwarantują pokrycie, ponieważ są one ważnym elementem ochrony w głąb i mają pewne możliwości, których nie mogą zapewnić oparte na sieci GSD. Ponieważ mobilność i wszechobecny dostęp do informacji są głównymi tematami otaczającymi dzisiejsze środowiska osobiste i biznesowe, ochrona na poziomie hosta jest zawsze obecna. Przejście hosta od polegania na środkach bezpieczeństwa sieci do kontekstu lokalnego i środków bezpieczeństwa uwzględniających środowisko zapewni solidniejsze i bardziej elastyczne zabezpieczenia, gdziekolwiek się znajduje. Bezpieczeństwo oparte na hoście - oprócz podstawowego firewalla - ma dodatkową złożoność i uwarunkowania ze względu na wymagania ochrony dodatkowych elementów (oprogramowania, usług itp.). Zdolność hosta do zrozumienia swojego lokalnego środowiska zapewnia bardziej szczegółową ochronę i widoczność. Zamiast skupiać się wyłącznie na dostępie do sieci opartym na portach, kontekst zwiększania środowiska definiuje, jakie aplikacje i usługi mogą: uzyskiwać dostęp do ruchu sieciowego lub odbierać go, uzyskiwać dostęp do innych usług lub zmieniać je lub wykonywać kod na maszynie wirtualnej (VM) w celu weryfikacji oczekiwanych zachowań.

Platformy zapór ogniowych … i Przyjaciele

GSD nadal rozwijają się pod względem formy, funkcji i zrozumienia kontekstu, aby zapewnić egzekwowanie dozwolonych ścieżek na wszystkich warstwach stosu sieciowego. Złośliwi aktorzy nadal tworzą coraz bardziej ukierunkowany i skuteczny kod, który porusza się po dozwolonej ścieżce. Te bardziej szczegółowe wymagania dotyczące inspekcji sieci powodują, że każda organizacja wybiera najbardziej odpowiednią platformę, aby spełnić jej potrzeby w zakresie bezpieczeństwa i wydajności.

Urządzenia trasujące.

Wraz ze wzrostem potrzeby przesyłania danych w obrębie sieci i poza nią, dostosowano urządzenia rutujące, aby zapewnić natywne, a następnie modułowe usługi bezpieczeństwa.

Listy kontroli dostępu.

Listy ACL urządzeń rutujących zazwyczaj zapewniają podstawowe egzekwowanie dozwolonych ścieżek przy minimalnym wpływie na wydajność. Listy ACL zezwalają na pojedyncze pakiety sieciowe lub odrzucają je na podstawie kombinacji parametrów z nagłówka, takich jak źródłowe i docelowe adresy IP i / lub port TCP / UDP. Usługi zabezpieczeń oparte na urządzeniach routingu dojrzały, aby zapewnić rozszerzone możliwości w oparciu o kontekstowe rozumienie sieci. Urządzenia routingowe mogą obsługiwać kilka technik inspekcji stanowej, z których najbardziej podstawową jest możliwość śledzenia połączeń wyłącznie na podstawie flag potwierdzenia (ACK) ustanowionego połączenia. Jednak ta metoda jest bardziej podatna na sfałszowane pakiety skierowane do zamierzonego celu niż tradycyjna inspekcja stanowa oparta na tabeli nawiązanych połączeń. Platformy routingu mogą również zapewniać funkcje ochrony przed spoofingiem w oparciu o topologię sieci. Po włączeniu urządzenie rutujące będzie podejmować decyzje o przekazywaniu na podstawie zrozumienia połączonych i wyuczonych tras i zezwala tylko na źródłowe adresy IP pochodzące z odpowiedniego interfejsu.

Moduły sprzętowe.

Wraz ze wzrostem przepustowości do dziesiątek do setek gigabitów na sekundę (i więcej), producent urządzeń rutujących musiał przenieść funkcje bezpieczeństwa do dedykowanego modułu (lub karty liniowej) dla konkretnego dostawcy. Moduł zapewnia logiczną ochronę dla jednej lub więcej dozwolonych ścieżek podczas korzystania z płyty montażowej w celu osiągnięcia wyższych szybkości transmisji danych i zapewnienia ochrony w oparciu o jedną lub więcej architektur zapór opisanych powyżej. Niektórzy dostawcy usług routingu obsługują również moduły podobne do serwerów kasetowych, co pozwala innym dostawcom zabezpieczeń na głębszą integrację ich technologii z infrastrukturą routingu.

Urządzenia.

Urządzenie GSD pojawiło się jako sposób na przeniesienie skomplikowanych decyzji dotyczących bezpieczeństwa z urządzeń routingowych na dedykowaną platformę bezpieczeństwa. Czynniki kształtu, możliwości i ograniczenia urządzeń różnią się w zależności od dostawców GSD, ponieważ aplikacja GSD jest zintegrowana z wybraną platformą sprzętową.

Prawnie zastrzeżony.

Opatentowany sprzętowy producent urządzeń GSD jest w stanie ustanowić i utrzymać ścisłą kontrolę nad wszystkimi aspektami platformy. Sprzęt jest specjalnie zaprojektowany do współpracy z oprogramowaniem GSD i zapewnia różne poziomy wydajności i funkcjonalności. Komponenty o wysokiej wydajności, takie jak zestawy instrukcji specyficznych dla aplikacji, są zwykle zastrzeżone. Jednak sprzedawca zrównoważy efektywność kosztową platformy, wybierając komercyjny sprzęt z półki (COTS) dla komponentów użytkowych (np. Interfejsy sieciowe i pamięć RAM). Towarzyszący, zastrzeżony, specyficzny dla sprzętu system operacyjny (OS) pozwala dostawcy zachować ścisłą kontrolę nad współdziałaniem, konfiguracją i wersjami oprogramowania.

Niezależne od sprzętu.

Niezależne od sprzętu urządzenia GSD przenoszą na klienta odpowiedzialność za zakup sprzętu, który spełnia określony zestaw wymagań, jednocześnie pozwalając dostawcy GSD zachować odpowiedzialność za rozwój aplikacji GSD i / lub systemu operacyjnego. GSD używa albo dostosowanej wersji systemu operacyjnego (zwykle Linux lub Berkeley Software Distribution [BSD]), albo instaluje się bezpośrednio na podstawowym systemie operacyjnym dostarczonym przez klienta. Aplikacja GSD zainstalowana na zastrzeżonym (lub wstępnie zmodyfikowanym) systemie operacyjnym zmniejsza natywne zagrożenia bezpieczeństwa dzięki niestandardowemu wzmocnieniu mechanizmów systemu operacyjnego przez dostawcę w celu usunięcia nieistotnych funkcji i funkcjonalności przy jednoczesnym zachowaniu ścisłej kontroli opisanej w powyższej sekcji. TheGSDapplication może być również w stanie zainstalować na określonych wersjach wybranego przez klienta natywnego systemu operacyjnego, zapewniając klientowi największą elastyczność w wyborze urządzenia GSD. Aplikacja GSD wprowadzi pewne zmiany zaostrzające, ale pozostawi większość zarządzania systemem operacyjnym klientowi. Zwiększa to ryzyko niezabezpieczonych i / lub źle działających implementacji ze względu na to, że dostawca GSD nie kontroluje w pełni konfiguracji systemu operacyjnego, poprawek i interoperacyjności.

Miękkie urządzenie

To miękkie urządzenie rozszerza niezależny od sprzętu / zastrzeżony system operacyjny GSD w platformę rozruchową, która może działać na sprzęcie klasy konsumenckiej. Ta platforma jest bardziej dostosowana do potrzeb w zakresie ochrony w określonym momencie, takich jak awaria głównego urządzenia GSD, szybkie wdrożenia i testy. Przed wdrożeniem miękkiego urządzenia klient musi złagodzić potencjalną „elastyczność" tego rozwiązania innymi względami, takimi jak łatwość zarządzania (konfiguracja, logowanie itp.), Skalowalność i wymagana funkcjonalność.

Urządzenie wbudowane.

Oprócz wysokiej klasy, skalowalnych urządzeń, dostawcy GSD dostrzegli również możliwość obsługi innych rynków, takich jak zapewnienie wyspecjalizowanych możliwości na platformach skalowanych w celu zaspokojenia potrzeb konsumentów oraz małych i średnich firm (SMB). Małe i średnie firmy rzadziej mają wystarczające fundusze lub dedykowany personel ds. Bezpieczeństwa do zakupu, zarządzania i monitorowania wielu urządzeń bezpieczeństwa. Moduły GSD klasy SMB zapewniają bardziej ekonomiczne urządzenie typu „wszystko w jednym" ze względu na mniejszy rozmiar, uproszczony interfejs użytkownika i mniejsze wymagania dotyczące wydajności. Oprócz standardowych opcji łączności przewodowej i / lub bezprzewodowej, urządzenie zazwyczaj zapewnia pełny zestaw funkcji bezpieczeństwa UTM.

Wirtualizacja

Dostawcy GSD oferują obecnie rozwiązania, od wykorzystania środowiska wirtualnego w celu zapewnienia niezależnych funkcji bezpieczeństwa sieci, po osadzanie szczegółowych zabezpieczeń na poziomie hiperwizora. Zamiast wymagać pełnej instalacji, niektórzy dostawcy GSD dostarczą preinstalowane urządzenie wirtualne, które minimalizuje całkowity czas wdrożenia. Ważne jest, aby upewnić się, że zwirtualizowany GSD zachowuje priorytet w pozyskiwaniu i utrzymywaniu zasobów z instancji maszyny wirtualnej. GSD obsługujący maszyny wirtualne działa jako niezależna jednostka bezpieczeństwa sieci. Zamiast posiadania dedykowanego sprzętu, GSD wykorzystuje warstwę abstrakcji sprzętu hiperwizora, aby uzyskać dostęp do niezbędnych zasobów. Ta implementacja zapewnia funkcje podobne do urządzeń sprzętowych do kontrolowania dozwolonych ścieżek na podstawie tego, jakie sieci kierują przez instancję maszyny wirtualnej GSD. Urządzenie wirtualne GSD z wbudowaną maszyną wirtualną integruje się z hiperwizorem w celu uzyskania niskiego poziomu dostępu do całego hosta / klastra maszyny wirtualnej. GSD ma teraz wgląd w wcześniej niedostępne

ścieżki komunikacyjne i jest w stanie przeprowadzić egzekwowanie dozwolonych ścieżek zarówno dla komunikacji między maszynami wirtualnymi, jak i wewnątrz nich.

Agenci na hoście

Ponieważ urządzenia mobilne wymagają większego dostępu do sieci wewnętrznej, w tym danych, które mają być przechowywane lokalnie na urządzeniu, tak samo wymagało się, aby te zabezpieczenia oparte na hoście były w stanie zminimalizować dodatkowe ryzyko zezwalania na taki dostęp. Możliwości antywirusowe, chociaż prawdopodobnie tylko marginalnie skuteczne w walce z nowymi i pojawiającymi się zagrożeniami, nadal są niezbędne do filtrowania znanych wektorów ataków. Funkcje zapory ogniowej na poziomie sieci i aplikacji zmniejszają profil zagrożeń sieciowych hosta. Host Intrusion Prevention System (HIPS) zapewnia ochronę przed znanymi i potencjalnie nieznanymi zagrożeniami ze względu na możliwość inspekcji aż do warstwy aplikacji. Gdy urządzenia zabezpieczające sieć nie wykrywają zagrożenia, ochrona oparta na hoście ma dodatkowe środki do wykrywania lokalnych anomalii ze względu na zwiększoną świadomość kontekstową tego, jak host - aplikacje i system operacyjny - powinien zachowywać się, zapewniając w ten sposób hostowi przewagę w wykrywanie pojawiających się zagrożeń. Organizacje nie powinny jednak lekceważyć kosztów administracyjnych niezbędnych do zarządzania tą ochroną i jej monitorowania.

MECHANIZMY BEZPIECZEŃSTWA SIECI.

Bezpieczeństwo sieci, niegdyś synonimem zapory, nadal rośnie zarówno pod względem zakresu, jak i głębokości. Rząd i organizacje wymagają, aby zabezpieczenia były wbudowane w systemy i rozwiązania, które produkują lub kupują. Jest całkowicie możliwe, że atak pochodzący z systemu nie pokrywa się z bezpośrednim atakiem obwodowym. Te wektory ataku obejmują prawdopodobne ekspozycje, na przykład urządzenie mobilne pracownika zainfekowane złośliwym kodem podczas podróży; nowy pendrive USB, który pracownik otrzymuje na konferencji; lub dostawca zapewniający legalne wsparcie, które podłącza jego / jej laptopa do sieci wewnętrznej. Ci, którzy wybierają systemy bezpieczeństwa sieci, muszą być w stanie rozszyfrować hiperbolę z rzeczywistości, aby upewnić się, że wdrożone urządzenie (a) realistycznie odpowiada (-ym) na określone ryzyko związane z organizacją. Urządzenia zabezpieczające bramy zachowują swoje podstawowe dziedzictwo kontroli dozwolonych ścieżek, ale teraz są znacznie bardziej zaawansowane pod względem zdolności do integracji ochrony w ładunku i poza nim.

Dozwolone ścieżki.

Urządzenia zabezpieczające sieć zapewniają ochronę dozwolonych ścieżek, aby zapewnić przepływ ruchu sieciowego tylko w oczekiwany i zamierzony sposób. Niestety, ten podstawowy poziom wymuszania jest niewystarczający, ponieważ ataki w warstwie aplikacji (np. Exploity przeglądarki po stronie klienta) wykorzystują te tradycyjne dozwolone ścieżki. Wymogi dotyczące bezpieczeństwa i zgodności z przepisami również napędzają wdrażanie bardziej wydajnych mechanizmów egzekwowania dozwolonych ścieżek głębiej w sieci wewnętrznej w celu ochrony własności intelektualnej, danych klientów / partnerów i przemysłowych systemów kontroli (ICS). Aby efektywnie zarządzać ryzykiem dozwolonych ścieżek, organizacje muszą zdefiniować i oprzeć swoje oczekiwane przepływy ruchu zarówno wewnętrznie, jak i zewnętrznie. Linia bazowa jest niezwykle ważna, gdy jedyną oznaką kompromisu może być nietypowa - choć pozornie łagodna - interakcja między

Tunelowanie.

Tunelowany dostęp do sieci wewnętrznej w celu zdalnego dostępu, wymiany informacji i handlu jest niezbędny dla większości organizacji. Te tunele, zwykle w postaci wirtualnej sieci prywatnej (VPN),

wykorzystują szyfrowanie w celu ochrony poufności przesyłanych danych. Jeśli GSD nie kończy tunelu, zwykle zapewnia tylko wymuszenie dozwolonej ścieżki sieci i warstwy transportowej do punktu końcowego zakończenia. Ten scenariusz fragmentuje inspekcję hermetyzowanego ruchu, wymagając od punktu końcowego samego zakończenia lub innego urządzenia zabezpieczającego po odszyfrowaniu, aby zapewnić dodatkową ochronę poprzez wymuszanie dozwolonych ścieżek i inspekcję warstwy aplikacji.

Ochrona przed podszywaniem się.

Jedną z najczęściej wykorzystywanych luk w protokole IP jest spoofing. Z powodu tej nieodłącznej słabości protokołu IPv4 hosta , stos sieciowy może generować pakiety, które mogą wyglądać na pochodzące z dowolnego wybranego adresu IP i / lub portu. Ten atak jest próbą oszukania hosta odbierającego i / lub jakiejkolwiek ochrony sieciowej pomiędzy nimi, tak aby uwierzył, że host, z którego pochodzi, podąża dozwoloną ścieżką. Ze względu na prostotę wykonywania ataków typu spoofing, dostawcy GSD opracowali i wdrożyli kilka skutecznych metod udaremniania tego typu ataków. Topologia sieci jest kluczowym elementem zdolności GSD do określenia, jaki ruch powinien pochodzić z każdego z jego fizycznych i / lub logicznych interfejsów. Jedną z powszechnych metod ochrony przed spoofingiem jest jawna definicja topologii sieci dla poszczególnych interfejsów. Zapewnia to wydajną metodę określania przez GSD, czy źródłowy adres IP pakietu wchodzący do interfejsu jest zgodny z tym, co GSD spodziewa się być siecią źródłową. Jeśli nie, pakiet nie spełnia kryteriów i jest odrzucany. Chociaż proste i efektywne, wadą jest ręczne zarządzanie definicjami sieci dla poszczególnych interfejsów. Inną metodą jest poznanie topologii sieci poprzez wykorzystanie tablicy routingu do podejmowania tego samego typu decyzji dotyczących ochrony przed fałszowaniem dla poszczególnych interfejsów. Zapora przechodzi ten sam proces oceny, czy źródłowy adres IP pakietu pasuje do tego, co powinno pochodzić z tego interfejsu. Nie wymaga to jednak ciągłej ręcznej interwencji w przypadku wystąpienia zmian w sieci, ponieważ silnik routingu aktualizuje te informacje. Chociaż ta metoda powoduje mniejsze obciążenie administracyjne, dwie wady obejmują problemy, jeśli sieć korzysta z routingu asymetrycznego i / lub padnie ofiarą ataku zatruwania tras. Oba te środki zapobiegające podszywaniu się są bardzo skuteczne przy ocenie, czy ruch sieciowy pochodzi z odpowiedniego interfejsu. Jednak koncentrujemy się wyłącznie na zapobieganiu naruszeniom adresu sieci wewnętrznej. Ponieważ nie wszystkie istniejące sieci IP są faktycznie przydzielone i / lub używane, te sieci „bogon” są kolejną metodą przeprowadzania ataków podszywających się. Ponieważ ruch sieciowy „bogon” pochodzi z interfejsu zewnętrznego, GSD nie blokowałby tego w oparciu o wspólne zasady zapobiegania fałszowaniu. Zaktualizowane listy są łatwo dostępne, co pozwala administratorowi bezpieczeństwa na egzekwowanie zabezpieczeń typu „bogon”. Niektóre GSD mają funkcję, która automatycznie aktualizuje listę w sposób cykliczny, zapewniając automatyczną ochronę

Tłumaczenie adresów sieciowych.

Translacja adresów sieciowych (NAT) to mechanizm, który odwzorowuje wewnętrzne (zwykle prywatne RFC 1918) adresy sieciowe na jeden lub więcej publicznych adresów IP. Jest to podstawowa funkcja w IPv4 ze względu na rosnący niedobór adresów, które można rutować publicznie. Ze względu na możliwość maskowania adresowania sieci wewnętrznej, NAT szybko stał się uważany za mechanizm bezpieczeństwa. Realistycznie, NAT zapewnia, że tylko ruch sieciowy zachowuje swoje tłumaczenia, ale nie ma wbudowanych funkcji bezpieczeństwa, takich jak kontrola ładunku. Aby zapewnić trwałe połączenia w architekturach wysokiej dostępności, NAT musi ustanowić i utrzymywać zsynchronizowaną kopię tabeli translacji z każdym składnikiem wysokiej dostępności. Ten mechanizm jest zgodny z tym samym połączeniem szeregowym lub sieciowym, które jest używane do obsługi tabeli stanów.

Wykrywanie wtargnięcia.

GSD z natury zapewniają kontrolę detektywistyczną na wielu poziomach. Te odrębne mechanizmy kontroli (np. Zapora ogniowa, system wykrywania / zapobiegania włamaniom itp.) Zapewniają lepszy wgląd w rodzaje i zakresy potencjalnych incydentów, gdy są odpowiednio skonfigurowane i monitorowane. Funkcje rejestrowania i ostrzegania związane z każdą kontrolą są ważnymi i niezbędnymi mechanizmami, z których pracownicy ochrony powinni korzystać w celu zrozumienia aktualnego stanu granicy. przed, w trakcie i po incydencie zapewnić terminowe i dokładne przeglądy dzienników. Bez takich przeglądów łatwo przeoczyć takie kwestie, jak ruch związany z atakiem i po ataku oraz błędne konfiguracje systemu. Dzienniki zapewniają również doskonałą okazję do dostrajania GSD, w tym optymalizacji baz reguł i redukcji fałszywych alarmów (po weryfikacji). Niezbędne są odpowiednio zaplanowane i skonfigurowane mechanizmy ostrzegania i logowania. Jeśli są źle wykonane, mechanizmy te mogą przeładować personel pomocniczy niepotrzebnymi lub nieistotnymi informacjami, sprawiając, że są oni mniej wydajni i skuteczni w rozwiązywaniu rzeczywistych problemów z bezpieczeństwem.

Zapobieganie / reagowanie na włamania.

Chociaż dzienniki i alerty są przydatne do wykrywania i badania incydentów związanych z bezpieczeństwem, mechanizmy te są pasywne i nie zapewniają ochrony przed zagrożeniami. Firewalle ewoluowały tak, aby obejmowały automatyczne, aktywne mechanizmy reagowania na zdarzenia związane z bezpieczeństwem i zapewniające. aktywną ochronę

Zakończenie połączenia.

Istotą ochrony obwodowej jest ochrona sieci wewnętrznej poprzez blokowanie prób połączeń, które nie są zgodne z ustalonymi zasadami dozwolonych ścieżek. Jedną z metod dla protokołów opartych na TCP jest udzielenie inicjatorowi (a czasem zamierzonemu odbiorcy) pakietowi resetowania (RST), przerywając połączenie. Najpopularniejszą metodą - która działa w przypadku protokołów zorientowanych połączeniowo i bezpołączeniowych - jest odrzucenie pakietu bez odpowiedzi. Jako zapory ogniowe ewoluowała w bardziej funkcjonalne GSD, ta ochrona została rozszerzona o blokowanie w oparciu o złośliwą aktywność występującą w warstwie aplikacji. I odwrotnie, atakujący mogą używać kończenia połączenia jako metody określania, gdzie i jakiego typu urządzenia zabezpieczające sieć są używane. Ten kontekst może zapewnić im dodatkowy wgląd w potencjalne metody omijania i / lub niekorzystnego wpływu na platformę bezpieczeństwa. Chociaż ta sytuacja jest nieunikniona bez względu na zastosowany mechanizm zakończenia, jest to kolejny powód, aby zastosować zabezpieczenia warstwami.

Adaptacyjne ograniczanie zagrożeń.

Chociaż polityka GSD zapewnia główny mechanizm egzekwowania, dostawcy szybko zdali sobie sprawę, że jest to niewystarczające, ponieważ atakujący nieustannie opracowują dodatkowe metody udaremniania tych zabezpieczeń. GSD obejmują kilka ulepszonych możliwości, które pozwalają urządzeniu dostosować się do określonych warunków zagrożenia i zapewniają ukierunkowane zapobieganie. Ponieważ osoby atakujące stosują metody zmiany źródeł ataków w celu uniknięcia wykrycia, a stosowanie sztywnej strategii białej listy (najmniejszych uprawnień) nie zawsze jest praktyczne, organizacje zazwyczaj decydują się na używanie czarnych list jako dodatkowego poziomu ochrony. Niektóre GSD używają dynamicznych grup obiektów do aktualizowania tych list według z góry określonego harmonogramu, co pomaga zminimalizować obciążenie administracyjne. Użycie progów zapewnia GSD bardziej skuteczną metodę przeciwdziałania konsekwentnym atakom, które w przeciwnym razie podlegałyby tej samej ocenie opartej na zasadach dla każdej próby. Jednym z

typowych typów progów jest liczba / typ zdarzeń w określonym czasie (np. Całkowita liczba pakietów na sekundę lub x liczba pakietów na sekundę w wielu docelowych adresach IP). Po naruszeniu GSD zazwyczaj automatycznie blokuje cały ruch z pierwotnego adresu IP na z góry określony czas. Ten typ techniki adaptacyjnej wymaga dodatkowych zasobów przetwarzania i wymaga dostrojenia, aby zapewnić, że nie wpłynie to na legalne przepływy sieciowe. Będąc głównie urządzeniami obwodowymi, GSD zazwyczaj mają minimalny wgląd w wewnętrzną, zaufaną sieć. Jednak nowoczesne infrastruktury bezpieczeństwa mogą wykorzystywać wiele metod wykrywania zagrożeń w całej sieci, aby zapewnić bardziej kompleksową ochronę. Po wykryciu urządzenie może wykorzystać infrastrukturę zarządzania bezpieczeństwem do aktualizacji innych zasad dotyczących urządzeń zabezpieczających - automatycznie zapewniając dodatkową ochronę lub izolację. Ta funkcja integruje się również z zabezpieczeniami opartymi na hoście, aby zwiększyć ochronę sieci. Jeśli host wykryje zagrożenie w niezaufanej sieci, infrastruktura dowie się o tym i dostosuje zabezpieczenia sieciowe, zanim urządzenie połączy się z siecią wewnętrzną.

Działania na poziomie systemu.

Jako dodatkową warstwę ochrony, urządzenia zabezpieczające bramy zwykle mają wbudowane mechanizmy wykrywania i reagowania na zagrożenia dla samej platformy. Zgodnie z modelem niejawnej odmowy, wyjątkiem jest zachowanie zabezpieczenia przed niepowodzeniem (np. Zamknięcie zapory) i nieprzekazywanie ruchu. Jednak ponieważ ta automatyczna odpowiedź wpływa na funkcjonalność urządzenia zabezpieczającego, ważne jest, aby administrator zapoznał się z tą funkcją i przetestował ją przed wdrożeniem, aby upewnić się, że zachowanie odpowiedzi jest zgodne z potrzebami organizacji w zakresie ochrony i dostępności.

Inspekcja aplikacji.

Możliwość ochrony dozwolonych ścieżek w oparciu o kombinacje adresów IP i / lub portów zapewnia marginalne korzyści w połączeniu z rosnącą złożonością i konfigurowalnością protokołów. Wraz z ewolucją GSD rozwijała się również możliwość oceny i egzekwowania dozwolonych ścieżek w oparciu o warstwę aplikacji. Ta możliwość obejmuje zarówno podstawowe oceny protokołów, takie jak sprawdzenie zgodności z RFC, jak i bramy pełnej warstwy aplikacji. W zależności od typu protokołu warstwy aplikacji dedykowane urządzenie może być niezbędne w środowiskach o dużej pojemności, bezpieczeństwie i / lub niezawodności. WAF. Zapory aplikacji internetowych (WAF) zapewniają ukierunkowane egzekwowanie w ramach dozwolonej ścieżki HTTP (S), które mogą łatwiej wykrywać i zapobiegać typowym atakom na serwer Web, takim jak XSS i wstrzyknięcie SQL, i zazwyczaj mają dodatkowe możliwości ochrony bardziej złożonej sieci Web 2.0 (np. AJAX) i sieci Web protokoły usług (np. SOAP lub JSON). Możliwe jest również zabezpieczenie w inny sposób podatnych na zagrożenia serwerów sieci Web przed exploitami, pisząc reguły ochrony, które wykrywają i unieważniają ruch związany z atakami w warstwie aplikacji. Tworzenie reguł granularnych WAF jest również lepiej dostosowane do ochrony niestandardowych aplikacji internetowych. Serwery proxy. Proxy przekazujące wymusza wychodzące połączenia internetowe, przechwytując i kontrolując dostęp na podstawie takich kryteriów, jak identyfikator użytkownika, pora dnia i / lub biała lista / czarna lista. W zależności od typu i konfiguracji proxy przekazujące może albo pośredniczyć w połączeniu wychodzącym i wysyłać żądania w imieniu klienta, albo po prostu wymuszać określoną dozwoloną ścieżkę. Klasyczne serwery proxy przekazujące wymagają konfiguracji po stronie klienta, aby wymusić komunikację z Internetem. Przezroczysty proxy to przekazujący serwer proxy, który działa jako „bump-on-the-wire" - umieszczany w linii lub poza portem span - i zazwyczaj nie wymaga konfiguracji po stronie klienta. Z drugiej strony zwrotny serwer proxy zapewnia ochronę dozwolonych ścieżek przychodzących. Połączenie przychodzące kończy się na serwerze proxy, a sam proxy nawiązuje drugą połowę połączenia bezpośrednio z serwerem aplikacji. Będąc połączeniem obsługiwanym przez

brokera, zapewnia to dodatkową warstwę ochrony ruchu przychodzącego poprzez przepisywanie potencjalnie zniekształconych żądań i / lub uniemożliwianie bezpośredniej komunikacji z serwerem aplikacji. Tożsamość aplikacji. Oprócz źródłowego i docelowego adresu IP zapory sieciowe zwykle polegają na porcie docelowym w celu ostatecznego określenia dozwolonej ścieżki dla typowych protokołów (np. HTTP - port 80 TCP). Jednak ominięcie inspekcji górnej warstwy (np. Proxy lub WAF) jest trywialne, zmieniając port docelowy na coś, co omija kontrolę warstwy aplikacji, ale nadal podąża za dozwoloną ścieżką. Urządzenia zabezpieczające obecnej generacji muszą mieć możliwość profilowania całego ruchu sieciowego na podstawie typu aplikacji zamiast portu docelowego. Identyfikacja aplikacji musi być w stanie przeanalizować ruch i zrozumieć podsystemy / protokoły osadzone w głównym strumieniu komunikacji. Na przykład Skype nie tylko z natury zapewnia wideokonferencje, ale także usługi przesyłania plików i czatu. Dzięki dodatkom funkcjonalność można rozszerzyć na zdalne udostępnianie / sterowanie pulpitem. Posiadając ten szczegółowy poziom zrozumienia aplikacji, możliwe jest szczegółowe egzekwowanie jednego lub większej liczby podzbiorów protokołów. To profilowanie obejmuje również określanie wspólnych protokołów na nieoczekiwanych portach i zaszyfrowany ruch za pośrednictwem wspólnego protokołu zwykłego tekstu - zaszyfrowanego lub nie.

Szyfrowanie.

Ochrona poufności danych wrażliwych w ruchu stale rośnie ze względu na potrzebę zminimalizowania ryzyka narażenia danych osobowych / danych osobowych i / lub własności intelektualnej. Stwarza to wyraźną potrzebę zapewnienia egzekwowania dozwolonych ścieżek podczas korzystania z usług szyfrowania do lub przez GSD. Ze względu na złożoność obliczeniową protokoły szyfrowania mogą znacznie zmniejszyć przepustowość GSD bez odciążania usług szyfrowania na dodatkowe, wbudowane urządzenie lub dedykowane urządzenia zewnętrzne w celu spełnienia potrzeb szyfrowania. Integracja szyfrowania w sieci i przepływach aplikacji jest niezbędna do ochrony poufności danych w ruchu. Chociaż niekoniecznie złośliwe, te zaszyfrowane sesje zmniejszają skuteczność wszelkich sieciowych urządzeń zabezpieczających próbujących sprawdzić chronione ładunki. Oprócz typowego ruchu w sieci VPN i HTTPS, GSD musi także być w stanie zidentyfikować zaszyfrowaną komunikację niezależnie od portu lub usługi. Dwie główne metody kontroli ruchu szyfrowanego to bezpośrednie zakończenie i deszyfrowanie w locie. W pierwszej metodzie GSD kończy szyfrowane połączenie. Daje to możliwość zbadania niegdyś tunelowanej komunikacji. Po sprawdzeniu i jeśli jest to dozwolone, GSD może przekazać pozostałą część komunikacji po odszyfrowaniu lub ponownie zaszyfrować sesję, aby zachować ochronę poufności punktu końcowego. W drugiej metodzie GSD będzie używać zdeponowanych kluczy szyfrowania do pasywnego deszyfrowania przepływów sieciowych. Oprócz spełnienia dodatkowych wymagań dotyczących wydajności, aby przeprowadzić pasywne deszyfrowanie, inną możliwą słabością jest niemożność zapewnienia w pełni synchronicznych odpowiedzi na wykryte zagrożenie - potencjalnie umożliwiając złośliwemu ruchowi przez dozwoloną ścieżkę, zanim nastąpi wymuszenie.

VPN. Wirtualna sieć prywatna (VPN) to hermetyzowana sieć nakładająca się na istniejący zestaw sieci fizycznych i logicznych. Typowa implementacja sieci VPN dotyczy zdalnego połączenia klienta, umożliwiając autoryzowanemu użytkownikowi dostęp do sieci wewnętrznej przez zaszyfrowany tunel. Po ustanowieniu klienci VPN mogą uzyskać dostęp do wewnętrznych sieci i / lub systemów, jednocześnie chroniąc poufność połączenia. Sieci VPN typu „lokacja” umożliwiają autoryzowanym zdalnym lokalizacjom uzyskanie bezpośredniego dostępu do sieci wewnętrznej dla wielu użytkowników za pośrednictwem jednego połączenia. Ponieważ istnieje niewielka lub żadna kontrola, gdy systemy mobilne opuszczają granice sieci wewnętrznej, wierność urządzenia mobilnego jest problemem. Ryzyko naruszenia bezpieczeństwa na każdym poziomie - od fizycznego po system

operacyjny, aplikacje i poza nim - może narazić sieć wewnętrzną na zwiększone ryzyko podczas sesji VPN. gdy niezaszyfrowany ruch opuszcza urządzenie kończące VPN - zobacz sekcję Wdrażanie, aby uzyskać dodatkowe informacje i uwagi. Przyśpieszenie. Używanie Secure Sockets Layer (SSL) i Transport Layer Security (TLS) do ochrony ruchu opartego na sieci Web lub IPsec do ochrony VPN stanowi potencjalną barierę dla kompleksowego egzekwowania dozwolonych ścieżek. Ponieważ zaszyfrowany ruch potencjalnie fragmentaryczny umożliwiał wymuszanie ścieżek, GSD ewoluowały, aby móc przerywać te połączenia w celu dodania dodatkowej warstwy inspekcji. Jednak szyfrowanie / deszyfrowanie jest matematycznie intensywne i wymaga wystarczających zasobów przetwarzania, aby to zapewnić procesy nie wpływają na przepustowość GSD. Kiedy GSD musi zakończyć lub sprawdzić zaszyfrowany ruch, powszechną metodą odciążenia tego przetwarzania i zminimalizowania wpływu na inny ruch przepływający przez GSD jest użycie sprzętowego modułu szyfrowania.

Egzekwowanie oparte na tożsamości.

Dzięki integracji z usługami katalogowymi przedsiębiorstwa przy użyciu takich mechanizmów, jak protokół LDAP (Lightweight Directory Access Protocol) lub usługa zdalnego dostępu telefonicznego (RADIUS), GSD mogą podejmować decyzje na podstawie tożsamości. Zamiast zezwalać lub odmawiać dostępu do dozwolonej ścieżki przez źródłowy adres IP, GSD może autoryzować dostęp dla każdego użytkownika lub na podstawie członkostwa w grupie i umieszczać te dane autoryzacyjne w dziennikach. Te dodatkowe szczegóły zwiększają możliwości raportowania i inspekcji, dostarczając bardziej szczegółowych informacji o określonym połączeniu, znacznie wykraczających poza adres IP lub nazwę DNS hosta żądającego przejścia przez dozwoloną ścieżkę.

Złożone silniki protokołów.

Złożone protokoły, w tym te używane do dostarczania bogatych w funkcje aplikacji internetowych, telefonii IP lub wyspecjalizowanych protokołów, takich jak te używane w przemysłowych systemach sterowania (ICS), są nieodłączną koniecznością dla wielu organizacji. Ze względu na stale rosnącą potrzebę udostępniania informacji i dostępu bez względu na wielkość lub lokalizację urządzenia mobilnego, te złożone protokoły przechodzą przez GSD. Nawet po pomyślnym wykryciu aplikacji będącej w użyciu, GSD jest w stanie zrozumieć i egzekwować zawiłości każdego protokołu w ciągłym wyścigu rozwojowym. Dzisiejsze aplikacje internetowe nieustannie rozwijają nowe funkcje, aby sprostać wymaganiom klientów. Media społecznościowe Strony internetowe oferują realne modele biznesowe i mogą wymagać od niektórych lub wszystkich użytkowników w organizacji dostępu do tej usługi w celu prowadzenia działalności. Ze względu na stale obecne elementy osobiste (np. Czat / komentarze, gry itp.) GSD musi być w stanie przeanalizować połączenie i selektywnie zezwolić na niektóre lub wszystkie funkcje oferowane przez aplikację hosta. Protokoły telefonii IP, takie jak protokół inicjacji sesji (SIP) i protokół czasu rzeczywistego (RTP), są zwykle nietolerancyjne dla opóźnień i jittera, które są wprowadzane przez GSD. Protokoły ICS wprowadzają zależności / zawiłości protokołów specyficzne dla danego producenta i są jeszcze mniej tolerancyjne na zmiany w sieci. Utrata lub spowolnienie komunikacji ICS może być tak poważne, jak uszkodzenie sprzętu lub śmierć podczas wpływania na systemy bezpieczeństwa. Chociaż wewnętrzna lub zewnętrzna granica sieci jest logicznym punktem inspekcji, GSD niekoniecznie jest odpowiednim urządzeniem do przeprowadzania takich szczegółowych kontroli protokołu. Zamiast tego sytuacje te mogą uzasadniać dodatkowe warstwy bezpieczeństwa przy użyciu wyspecjalizowanych urządzeń do egzekwowania warstwy aplikacji lub protokołów specjalnych.

Kontrola treści i zapobieganie wyciekom danych.

Polityka organizacji określa oczekiwania behawioralne jej pracowników. Zasady dopuszczalnego użytkowania (lub o podobnej nazwie) zazwyczaj obejmują kwestie specyficzne dla korzystania z

zasobów technologicznych; jednak sama polityka nie może zapewnić aktywnej ochrony. Filtrowanie treści (CF) wypełnia lukę między technicznym a nietechnicznym egzekwowaniem polityki. To wymuszanie zwykle koncentruje się na wewnętrznych użytkownikach próbujących uzyskać dostęp do zasobów informacyjnych poza organizacją. Dzięki filtrowaniu często używanych protokołów, takich jak HTTP i SMTP, organizacja może zminimalizować dostęp użytkowników do informacji, które nie pasują do definicji zastosowań biznesowych. Ta technologia ma kilka metod sprawdzania, klasyfikowania i filtrowania treści. Inspekcja przybiera różne formy, w tym przebywanie w linii, poza pasmem w celu monitorowania ruchu przechodzącego bez wpływu na połączenie fizyczne lub w połączeniu z przekierowaniem proxy. Klasyfikacja odbywa się za pomocą wielu metod, w tym kategorii zdefiniowanych przez producenta, czarnych list i / lub punktacji reputacji na podstawie adresu IP i / lub nazwy DNS. Pozwala to również organizacji na wybranie podzbioru zasad dostarczania i / lub selektywne opracowanie białej listy, aby zapewnić bardziej szczegółowe egzekwowanie. Funkcja filtrowania rejestruje i / lub przerywa połączenia, umożliwiając organizacji dostosowywanie swojej reakcji na wykryte naruszenia zasad, w tym przekierowanie na stronę internetową „nie do użytku biznesowego" i / lub automatyczne powiadomienia administracyjne i / lub kierownicze o powtarzających się naruszeniach.

Klasyfikacja i egzekwowanie informacji.

Przeoczonym, ale ważnym aspektem zapewniania informacji jest właściwa klasyfikacja informacji / danych na kategorie. Pozwala to organizacji określić działania mające na celu zmniejszenie ryzyka niezbędne do ochrony każdego poziomu / typu informacji. Podobnie jak w przypadku procesu klasyfikacji stosowanego przez rządy, identyfikacja wrażliwych informacji zwiększa możliwość egzekwowania nie tylko tego, kto ma dostęp do informacji, ale także gdzie i jak te informacje mogą być przekazywane. Zarządzanie prawami cyfrowymi (DRM) i zapobieganie utracie danych (DLP) to dwie technologie obecnej generacji służące do radzenia sobie z tymi specyficznymi dla informacji zagrożeniami. DRM koncentruje się na definiowaniu i egzekwowaniu danych w stanie spoczynku, zazwyczaj na poziomie repozytorium informacji. GSD mogą obejmować zabezpieczenia DLP, takie jak wymuszanie ochrony danych w ruchu, w tym odmawianie przesyłania plików w oparciu o zawartość / przeznaczenie i / lub wymaganie szyfrowania danych wrażliwych.

Anty-malware.

Współczesny wektor ataku polega na atakowaniu powszechnie używanej witryny / usługi i wstrzyknięciu złośliwego oprogramowania. Chociaż filtr zawartości może podjąć początkową decyzję o zezwoleniu na połączenie w oparciu o konkretną nazwę witryny, może również mieć dodatkową możliwość przechwytywania i blokowania złośliwej zawartości, zanim dotrze ona do hosta. Ta funkcja umożliwia ocenę różnych typów ruchu, takich jak załączniki SMTP i pobieranie HTTP. Chociaż ten rodzaj ochrony warstwy aplikacji może radykalnie zmniejszyć przepustowość GSD, możliwe jest przekierowanie skanowania do dodatkowego modułu w GSD z dedykowaną mocą przetwarzania lub do dedykowanego sieciowego urządzenia chroniącego przed złośliwym oprogramowaniem.

Aktywna zawartość.

Aktywny kod używany w połączeniach HTTP - taki jak Silverlight, Java, AJAX i Flash - stanowi podstawę bogatego doświadczenia internetowego ale także zwiększa zagrożenie bezpieczeństwa ze względu na ich funkcjonalność ukierunkowaną na aplikacje. Złośliwe załączniki do wiadomości e-mail - takie jak dokumenty z osadzonym kodem - są częstymi składnikami kampanii phishingowych i spamowych. W połączeniu z zabezpieczeniami opartymi na hoście, GSD może zmniejszyć ryzyko aktywnego kodu, uniemożliwiając określonym typom kiedykolwiek dotarcie do punktu końcowego i / lub skanowanie

aktywnego kodu w piaskownicy przed zezwoleniem aktywnemu kodowi na przejście przez dozwoloną ścieżkę.

Buforowanie

Chociaż łączny koszt przepustowości nadal spada, organizacje nadal szukają możliwości wydajniejszego zarządzania tymi często przeciążonymi obwodami. Serwery proxy zazwyczaj integrują mechanizmy buforowania, aby lokalnie przechowywać często używaną zawartość internetową, zwiększając lokalną przepustowość poprzez zmniejszenie ruchu związanego z Internetem. GSD może być również w stanie świadczyć podobne usługi buforowania, mając wystarczającą pojemność pamięci i zasoby przetwarzania.

IPv6.

Przydzielenie ostatnich pozostałych dostępnych bloków adresów IPv4 do regionalnych rejestrów internetowych (RIR) nastąpiło w 2011 r., Wskazując, że na świecie nie ma adresów IPv4. Chociaż można argumentować, że stwierdzenie to jest zbyt dramatyczne, masowa migracja do IPv6 nadal odbywa się w wolniejszym tempie niż można by się spodziewać, mimo że IPv6 został opracowany pod koniec lat 90. Chociaż organizacje nadal opracowują swoje indywidualne plany przejścia, prawdopodobnie IPv6 jest już w ich środowisku. Wiele nowoczesnych systemów operacyjnych i urządzeń ma podwójne stosy sieciowe IPv4 i IPv6, z których niektóre są domyślnie włączone. Protokół IPv6 i powiązane z nim technologie przejściowe mają określone konsekwencje dla bezpieczeństwa, które GSD musi zrozumieć i egzekwować.

Obawy dotyczące bezpieczeństwa granic.

Adresowanie. Protokół IPv6 jest bardziej elastyczny w podejściu do adresowania dynamicznego. Zamiast polegać wyłącznie na protokole DHCP, urządzenie IPv6 może adresować się za pomocą bezstanowej automatycznej konfiguracji adresów (SLAAC). Host używa unikalnego identyfikatora (zazwyczaj własnego adresu kodu uwierzytelniania wiadomości (MAC)) oprócz protokołu Neighbor Discovery (ND) w celu zakończenia automatycznego adresowania. Ponieważ nie ma wymogu uwierzytelniania, GSD musi zapobiegać próbom działania urządzeń zewnętrznych jako routera wewnętrznego podczas procesu adresowania. Znaczny wzrost liczby dostępnych adresów w dowolnej sieci IPv6 uniemożliwia wykrycie urządzeń i topologii sieci przy użyciu tradycyjnego skanowania portów. Korzystając z protokołu wykrywania grupowego nasłuchiwania (MLD), osoba atakująca może wysłać sondę na lokalny adres multiemisji (ff02 :: 1) i nasłuchiwać odpowiedzi. GSD musi blokować tę możliwość na obwodzie, aby uniemożliwić urządzeniom zewnętrznym próby wykrycia wewnętrznych hostów i topologii.

Tunelowanie

Bez wszechobecnej kompleksowej łączności IPv6 istnieje kilka technologii przejściowych IPv6 (takich jak 6to4 i Teredo), które umożliwiają systemom obsługującym protokół IPv6 tunelowanie komunikacji w starszych sieciach IPv4. Podobnie jak w przypadku innego ruchu tunelowanego, aby był skuteczny, GSD musi być w stanie nie tylko wymusić odpowiednią dozwoloną ścieżkę dla ruchu tunelowanego, ale także sprawdzać zahermetyzowany pakiet IPv6. IPv6 ma również natywną obsługę protokołu IPsec (zarówno AH, jak i ESP). Konfiguracja i korzystanie z IPsec w środowisku IPv6 wymaga tej samej dyscypliny w wybieraniu i konfigurowaniu opcji kryptograficznych, jak w przypadku IPv4. Możliwe jest również użycie IPv4 IPsec do ochrony tuneli technologii przejściowej IPv6, ponieważ w przeciwnym razie niezaszyfrowane sesje tunelowe byłyby narażone na przechwytywanie i / lub manipulację.

Globalna łączność

Translacja adresów sieciowych (NAT) jest istotnym elementem łączności internetowej IPv4 ze względu na stosunkowo „małą” liczbę publicznie routowalnych adresów. Rozmiar przestrzeni adresowej IPv6 (2^{128} adresów) zapewnia globalną łączność IP bez potrzeby (lub definicji) zastępowania NAT. Urządzenia IPv6 będą teraz ponownie komunikować się natywnie w ramach dynamiki obwodu zmieniającego Internet. Przy włączonym IPv6 istotne jest, aby GSD wymusiło ścisłe filtrowanie danych wejściowych i wyjściowych.

Mobilność

Mobilny protokół IPv6 (MIPv6) umożliwia hostom utrzymanie dostępu do sieci domowej podczas fizycznego roamingu do innych lokalizacji i niekontrolowanych sieci. Użytkownik mógłby opuścić sieć biurową i podróżować z jednego spotkania na drugie bez utraty łączności z siecią wewnętrzną. Ponieważ urządzenie może przenosić sieć do sieci bez przerywania połączenia wewnętrznego, MIPv6 stwarza również potencjalne problemy z inspekcją stanową, jeśli GSD nie rozumie protokołu. Jeśli organizacja zdecyduje się nie obsługiwać MIPv6, GSD powinien filtrować pakiety nagłówka routingu typu 2 (RH2).

Dodatkowe uwagi

Ochrona hosta.

Chociaż firewalle i GSD odgrywają kluczową rolę w ochronie całej infrastruktury sieciowej, rozmieszczenie tych urządzeń we wszystkich punktach w sieci nie jest ani opłacalne, ani możliwe. Poszczególne hosty muszą mieć sposób na ochronę przed zagrożeniami niezależnymi od urządzeń zabezpieczających sieć. W przeciwieństwie do sieci, host ma kontekstowe zrozumienie tego, co system może, co robi i / lub powinien robić. Oprócz prostej funkcji zezwalaj i odmawiaj, kontekstowe środki bezpieczeństwa mogą wykrywać nieoczekiwane zmiany konfiguracji systemu, takie jak zmiany usług lub nieoczekiwane zachowanie aplikacji. Gdy host opuszcza sieć wewnętrzną, staje się rozszerzeniem profilu ochrony sieci. Zapewniając odpowiednie lokalne zabezpieczenia na poziomie sieci i aplikacji, mobilny punkt końcowy pomaga złagodzić potencjalne problemy po ponownym połączeniu się z siecią wewnętrzną. Istotne jest również określenie wymaganego poziomu ochrony oraz tego, jak każdy z tych dodatkowych poziomów bezpieczeństwa wpłynie na wydajność systemu, zarządzanie i wpływ na użytkownika końcowego.

Sieć.

Hosty muszą być w stanie określić typy i stosowność ruchu przychodzącego i wychodzącego. Te ograniczenia sieciowe mogą się różnić w zależności od sieci wewnętrznej i sieci niekontrolowanych. W pewnych okolicznościach cały ruch sieciowy może być podejrzany i poddawany dalszej analizie. Na przykład w sieci wewnętrznej host zezwala na większość ruchu przychodzącego i wychodzącego. Gdyby host znajdował się w niekontrolowanej sieci, nie pozwoliłby na żadne nieustalone przepływy sieciowe. Proste zabezpieczenia sieciowe oparte na hostach nie wystarczą; dodatkowe mechanizmy ochrony hosta, takie jak zapobieganie włamaniom, mogą wykrywać i powstrzymywać ataki sieciowe i aplikacje.

Dostęp do aplikacji.

Znajomość kontekstowa hosta pomaga również dyktować zdolność aplikacji do wykonywania, a także wysyłania i / lub odbierania danych. Celem jest zapewnienie dostępu do sieci tylko odpowiednim aplikacjom i / lub usługom. Zasady ochrony hosta mogą zezwalać aplikacjom na nawiązywanie połączeń wychodzących, ale nigdy nie nasłuchują (ani nie akceptują nierozpoznanych pakietów przychodzących). Na przykład serwer HTTP używa demona do nasłuchiwania prób połączeń. Klient HTTP spróbuje

nawiązać połączenie z demonem serwera HTTP. Korzystając z mechanizmu ochrony hosta, można by zapobiec jednej lub obu z tych czynności.

Zabezpieczenia hybrydowe.

System zapobiegania włamaniom do hosta (HIPS) działa podobnie do systemu zapobiegania włamaniom sieciowym (NIPS), wykrywając znane wzorce ataków i / lub nietypowe zachowania. Hybrydowe zabezpieczenia hosta opierają się na świadomości kontekstowej hosta i zapewniają możliwość monitorowania innych nietypowych działań na poziomie aplikacji, takich jak zmiany w plikach binarnych, manipulacja usługami i uruchomione nasłuchiwania.

ROZLOKOWANIE

Architektura strefowa.

We współczesnej interpretacji architektury ekranowanej podsieci strefy definiują różne typy i / lub wrażliwości sieci, aplikacji i / lub usług. Zapewnia to możliwość zarządzania dozwolonymi ścieżkami na poziomie makr (na strefę) oprócz tradycyjnych dozwolonych ścieżek (określonych hostów lub usług). Ponieważ wymagania zwiększają bezpieczeństwo sieci, koncepcja strefowania jest równie skuteczna, gdy jest używana do zarządzania i ochrony sieci wewnętrznych i zewnętrznych.

Strefy obwodowe.

Router brzegowy stanowi pierwszą linię obrony architektury przed atakami zewnętrznymi. Listy ACL na tym routerze powinny odzwierciedlać podstawową konfigurację dozwolonych ścieżek interfejsu zewnętrznego (niezaufanego) firewalla i zapewniać kilka ważnych korzyści. GSD jest w stanie działać z optymalną wydajnością, ponieważ ruch odrzucony na podstawie reguł filtrowania pakietów routera granicznego normalnie nigdy nie dotarłby do zapory. Pozwala to firewallowi skupić się, pod względem obciążenia, na inspekcji protokołu. Jeśli na przykład zapora otrzyma pakiet, który nigdy nie powinien przejść przez listę ACL routera granicznego, zapora może założyć, że router nie działa normalnie. Zapora może wówczas odpowiednio zareagować, wykonując takie czynności, jak przerywanie wszystkich połączeń z określonego hosta.

Strefy usług zewnętrznych.

Konieczność mobilności i dostępności stawia istotne wymagania w stosunku do systemów połączonych z Internetem, a także zwiększa koszty administracyjne związane z zarządzaniem dostępem zewnętrznym. Poniższe sekcje zawierają jedynie próbkę możliwych architektur zewnętrznych stref usług.

Użyteczność.

Zamiast zrzucać systemy, takie jak Internet, DNS i poczta e-mail do jednej sieci, może być korzystne wdrożenie stref. Serwery narzędziowe, takie jak DNS i poczta e-mail, mogą logicznie znajdować się w tej samej sieci. Serwery internetowe zwykle wymagają większej przepustowości i dzięki tej koncepcji mogą chronić całą strefę za pomocą prostej reguły dostępu przychodzącego.

Extranet.

Systemy ekstranetowe stwarzają dodatkową złożoność, ponieważ zapewniają interfejs użytkownika, podczas gdy systemy wewnętrzne mogą zapewniać odpowiednią zawartość. Strefowanie zapewnia większą elastyczność, umożliwiając zewnętrznym połączeniom dotarcie do serwerów Extranet, zapewniając tym samym dostęp do zasobów wewnętrznych.

VPN.

Sieci VPN są również okazją do wykorzystania stref. Ponieważ urządzenie łączące VPN musi być połączone z Internetem, wymaga to dwóch różnych sieci podłączonych do zapory. Zewnętrzny interfejs z dostępem do Internetu (niezaufany VPN) zezwalałby tylko na kilka protokołów dla przychodzącego i wychodzącego zaszyfrowanego ruchu. Druga sieć (zaufana VPN) jest przeznaczona dla nieszyfrowanego ruchu sieciowego przenoszonego do iz sieci wewnętrznej. Architektura ta zapewnia również dodatkową ochronę sieci wewnętrznej w przypadku naruszenia bezpieczeństwa urządzenia VPN, a także tworzy punkt kontroli ruchu, który jest niezakłócony przez szyfrowanie.

Wewnętrzne strefy serwisowe.

Wraz z rosnącym rozpowszechnieniem aktywów niebędących własnością firmy i bardziej złożonymi przepływami danych organizacje nadal poszukują lepszych metod ochrony sieci wewnętrznych. Poniższe sekcje zawierają jedynie próbkę możliwych architektur wewnętrznych stref usług.

Systemy administracyjne i monitorujące: Organizacje zazwyczaj ograniczają bezpośredni dostęp do sieci i urządzeń zabezpieczających. Wymagając, aby cały ruch administracyjny i monitorujący pochodził z określonego hosta i / lub sieci, strefa może skutecznie zmniejszyć profil zagrożenia każdego urządzenia. Ta strefa pozwoliłaby nie tylko na minimalny ruch niewtajemniczonych , ale ograniczyłby również połączenia wychodzące do systemów zarządzanych i monitorowanych.

Systemy o wysokiej wartości: Organizacje polegające w dużym stopniu na własności intelektualnej i / lub innych chronionych typach danych (np. Danych osobowych i finansowych) mają nieodłączną potrzebę zapewnienia wyższego poziomu ochrony w celu ochrony swoich inwestycji. Podział na strefy zapewnia dodatkową warstwę ochrony poprzez zminimalizowanie niepotrzebnych przepływów informacji do / z tych cennych systemów

Systemy sterowania przemysłowego: Incydenty, takie jak Stuxnet i Night Dragon, przypominają nam, że chociaż niektóre typy systemów są uważane za niezwykle złożone i mniej dostępne, to tylko kwestia czasu, zanim uda się osiągnąć kompromis. Organizacje produkcyjne ze znacznymi inwestycjami w kontrolę przemysłową i

Systemy nadzoru i pozyskiwania danych (SCADA) mogą (lub mają wymagania) izolować te środowiska jako dodatkowy poziom ochrony i / lub zgodności.

Pozycjonowanie GSD.

Zwiększone wykorzystanie szyfrowanych protokołów, takich jak SSL / TLS i IPsec, może zaślepić zabezpieczenia sieciowe. Niektóre GSD mają możliwość kończenia zaszyfrowanych sesji, chociaż zwiększone wymagania dotyczące przetwarzania i przepustowości mogą przekroczyć ograniczenia urządzenia. W razie potrzeby architektura bezpieczeństwa powinna wdrażać odpowiednie środki zaradcze w strategicznych lokalizacjach, które unikają szyfrowanego ruchu. W ten sposób GSD może skupić się na swojej podstawowej roli wykrywania i zapobiegania złośliwej aktywności.

Inline.

Umieszczenie GSD w linii tworzy punkt dławienia dla aktywnego wymuszania dla całego ruchu sieciowego, który przez niego przepływa. Gdy złośliwy pakiet dotrze do GSD, analiza protokołu wykryje anomalię i nie pozwoli jej na przepływ przez inny interfejs. Chociaż ograniczenia przepustowości są typowym problemem, nieprawidłowo skonfigurowane urządzenia w linii mogą również stanowić warunek odmowy usługi. Przy odpowiednim planowaniu i wdrażaniu infrastruktury możliwe jest zminimalizowanie tych zagrożeń.

Kontrolowanie ruchu szyfrowanego.

Ponieważ urządzenia mobilne często wychodzą poza kontrolowaną sieć, jedno logiczne miejsce do oceny ruchu znajduje się po niezaszyfrowanej stronie połączenia. Może to znajdować się z tyłu terminatora SSL (w niektórych przypadkach na samym serwerze) lub po niezaszyfrowanej stronie połączenia VPN. Drugą opcją jest użycie GSD do inspekcji (np. Zakończenia i / lub biernego deszyfrowania) ruchu przed przekazaniem go do miejsca docelowego. Ten poziom funkcjonalności wymaga znacznych zasobów przetwarzania, ale może być konieczny, jeśli niższe poziomy bezpieczeństwa są niewystarczające.

STRATEGIE ZARZĄDZANIA I MONITOROWANIA.

Niezależnie od twierdzeń producenta, urządzenia zabezpieczające sieć nigdy nie są przedsięwzięciem typu „podłącz i używaj". Konieczne jest podjęcie dodatkowych kroków w celu zdefiniowania wymagań bezpieczeństwa w zakresie zarządzania i monitorowania komponentów GSD. Takie podejście pomaga zapewnić wszechstronną postawę bezpieczeństwa.

Monitorowanie.

Firewalle i GSD zapewniają złożoną funkcjonalność; monitorowanie takich systemów musi wykraczać poza zwykłe sprawdzanie dostępności systemu i obejmować stan urządzenia, dostępność i integralność.

Zdrowie.

Metryki, takie jak wykorzystanie procesora, dostępna pamięć RAM i liczba połączeń, mają wpływ na ogólną funkcjonalność. Scentralizowana konsola zarządzania może zapewniać możliwość monitorowania tych wskaźników i ostrzegania o nich. Jeśli ta funkcja jest niedostępna, może być konieczne użycie protokołów monitorowania, takich jak Simple Network Management Protocol (SNMP) i / lub Remote Monitoring (RMON), aby zebrać te statystyki. GSD musi ściśle ograniczyć systemy zdolne do sondowania przy użyciu tych metod ze względu na nieodłączną niepewność wyżej wymienionych protokołów monitorowania. Na podstawie trendów tych metryk można określić, kiedy należy zwiększyć przepustowość lub zakupić systemy, które są w stanie sprostać nowym wymaganiom dotyczącym przepustowości lub przetwarzania.

Dostępność.

Gdy GSD są niedostępne, funkcjonalność sieci może się dramatycznie zmniejszyć. Prosty test dostępności systemu polega na użyciu protokołu ICMP do „pingowania" jednego lub większej liczby interfejsów, aby upewnić się, że samo urządzenie odpowiada. Jednak takie podejście może być zwodnicze. To, że samo urządzenie odpowiada, nie oznacza, że prawidłowo przekazuje ruch. Wskazane jest również wysyłanie sond (np. ICMP, traceroute lub innych zapytań) do czegoś po drugiej stronie każdego interfejsu, aby upewnić się, że drugie urządzenie faktycznie odbiera pakiety, aby zapewnić prawidłowe wyniki. Takie podejście zapewnia lepszy ogólny obraz dostępności GSD.

Integralność.

Zdolność do zaufania komponentom systemów bezpieczeństwa sieci jest niezbędna. Możliwość złamania zabezpieczeń firewalla przez rootkita lub GSDis nowa rzeczywistość. Systemy te muszą mieć możliwość ochrony przed modyfikacjami komponentów systemu, takimi jak zaprzestanie działania i / lub powiadamianie o zmianie. Jeśli ta wbudowana funkcja byłaby niedostępna, można napisać skrypt do generowania kryptograficznych skrótów krytycznych składników systemu i weryfikowania ich względem znanej zaufanej wersji.

Zasady.

Zasada GSD jest podstawową definicją zapewniania i ochrony dozwolonych ścieżek. Większość systemów bezpieczeństwa przetwarza pakiety zaczynające się na początku polityki i kontynuowane do momentu dopasowania lub osiągnięcia końca bazy reguł (co powinno być jawnym „odrzuceniem wszystkich"). Scentralizowane konsole zarządzania zapewniają intuicyjne interfejsy GUI do konfigurowania i łatwego zarządzania jedną lub większą liczbą reguł zapory i GSD. Niektóre platformy zapewniają również możliwość zarządzania zasadami bezpośrednio z urządzenia.

Definiowanie dozwolonych ścieżek.

Dozwolone ścieżki identyfikują określone protokoły używane do realizacji komunikacji. W typowym środowisku internetowym usługi biznesowe wymagają dozwolonych ścieżek, takich jak HTTP (S), SMTP i DNS. Te wymagania będą się różnić, ale w środowisku każda dozwolona ścieżka powinna bezpośrednio odnosić się do wymaganej usługi. Zaczynając od niejawnej lub jawnej (w zależności od platformy) reguły „deny any", dozwolone ścieżki zostaną dodane jako reguły „allow", takie jak PERMIT HTTP, z określonymi w poniższych sekcjach. Chociaż adresowanie sieciowe nie zapewnia skutecznego uwierzytelniania systemów lub użytkowników, restrykcyjne punkty końcowe mogą znacznie utrudnić osobie atakującej wykorzystanie prostej w innym przypadku luki w zabezpieczeniach. Ważne jest również, aby dokładnie zidentyfikować punkty końcowe, szczególnie w przypadkach, gdy te punkty końcowe mogą znajdować się w strefach wewnętrznych, a nie ekstranetowych lub użytkowych. Kierunek ruchu wskazywany przez źródło zainicjowania połączenia jest przydatny przy definiowaniu reguł z kilku powodów. Po pierwsze, reguły mogą być tak napisane, że tylko odpowiedzi na wewnętrznie utworzone dozwolone ścieżki są wpuszczane ze strefy niezaufanej, zamiast jawnie zezwalać na protokół dwukierunkowy. Ponadto zapora może przetwarzać reguły w różnym czasie w zależności od projektu i / lub konfiguracji.

Złożoność zasad GSD.

Standardowe reguły zapory działają na prostych zasadach logicznych. Na przykład zezwalaj lub nie zezwalaj na ruch sieciowy przechodzący z hosta lub sieci X do Y na porcie Z. Złożoność wymagana od GSD oceniających ruch sieciowy jest znacznie większa. Na przykład ocena ta może być połączeniem testu logicznego w celu sprawdzenia, czy przychodzący adres e-mail pochodzi z zaufanego źródła, czy treść wiadomości jest akceptowalna i przeskanuje załącznik w poszukiwaniu wirusów. Administratorzy muszą rozumieć protokoły wyższego poziomu, aby zapewnić zgodność polityki GSD z oczekiwanymi i wymaganymi typami zabezpieczeń. Wraz ze wzrostem liczby i złożoności przepisów rosną wymagania dotyczące przetwarzania dla GSD. Poza podstawowymi funkcjami zapory, zasady GSD zazwyczaj obejmują wymuszanie dodatkowych środków bezpieczeństwa na podstawie reguły. Na przykład GSD używa tylko filtrowania sieci i / lub warstwy transportowej w celu ograniczenia dostępu do terminatorów VPN organizacji. Polityka może obejmować zabezpieczenia WAF, ale tylko dla stref użytkowych. Wchodzący i wychodzący ruch sieciowy i transfer plików może wymagać dodatkowej inspekcji NIPS. Chociaż ten poziom dostosowywania powoduje dodatkowe obciążenie administracyjne, selektywne (a nie ogólne) stosowanie dodatkowych zabezpieczeń w ten sposób może zmniejszyć wpływ dodanych zabezpieczeń na wydajność.

Zarządzanie zmianami.

Niezależnie od tego, czy zarządzasz jedną, czy setką polityk, istotnym elementem jest posiadanie procesu śledzenia zmian zasad. Zarządzanie zmianą może być uciążliwe, ale ma kilka zalet. Po pierwsze, zapewnia to wycofanie informacji, gdyby zmiana spowodowała problemy. Po drugie, zapewnia ścieżkę audytu tego, kto zażądał zmiany (i dlaczego), a także kto zmienił politykę. Wreszcie zapewnia metodę

usprawniania żądań zmian, zapewniając jedną metodę akceptowania, przeglądania, wdrażania i walidacji zmian zasad

Ocena wtórna.

Wprowadzanie zmian w zasadach jest zwykle prostym procesem, takim jak dodanie dostępu HTTPS do nowego serwera ekstranetu. Jednak im bardziej skomplikowana zmiana, tym większe prawdopodobieństwo wystąpienia błędów. Możliwość oceny proponowanej zmiany przez innego administratora zapewnia nową perspektywę, która może wyłapać niewielką rozbieżność, która może mieć negatywne konsekwencje. Kolejnym krokiem w procesie zarządzania zmianą jest walidacja w wielu grupach operacyjnych możliwość wykrycia potencjalnych konfliktów z innymi częściami infrastruktury w wyniku zmiany.

Audyty / testy.

Czy Twój firewall lub GSD działa zgodnie z oczekiwaniami? Czy GSD przechwytuje najnowszy załącznik zainfekowany złośliwym oprogramowaniem? Czy postawiłbyś na to przyszłość swojej organizacji? Te pytania są prostymi, ale potężnymi przypomnieniami, że należy sprawdzić, czy urządzenia zabezpieczające sieć działają zgodnie z oczekiwaniami. Oprócz bieżących i dogłębnych przeglądów dziennika, w odpowiedzi na te pytania pomoże odpowiedni zestaw audytów i testów. Ponadto konsole zarządzania powinny udostępniać dziennik audytu, który śledzi, kto wprowadza zmiany w dowolnej części środowiska. Ocena podatności i testy penetracyjne to skuteczne metody określania ważności reguł polityki. Na przykład zapora nie powinna zezwalać na połączenie HTTP z systemem z skonfigurowanym tylko dostępem SSL / TLS. Jeśli dostęp HTTP powiedzie się, czy wystąpił błąd testowanej reguły, czy istnieje inna reguła znajdująca się wyżej w bazie reguł błędnie zezwalająca na taki dostęp, czy też dzieje się coś nieoczekiwanego? Narzędzia i procesy muszą być gotowe, aby odpowiedzieć na te pytania, zanim zrobi to ktoś inny.

KONSERWACJA.

Instalowanie poprawek na stacjach roboczych i aktualizowanie definicji / sygnatur złośliwego oprogramowania to powszechne praktyki, ale ten proces jest jeszcze ważniejszy w przypadku systemów chroniących sieć. Konieczne jest przetestowanie ważności i stabilności każdej aktualizacji, aby mieć pewność, że błędne lub nieuczciwe zmiany nie przerywają operacji.

Poprawianie.

Żaden system nie jest z natury i nieskończenie bezpieczny i może być możliwe zniszczenie urządzenia zabezpieczającego ze względu na lukę w systemie. Konieczne jest monitorowanie witryn GSDWeb pod kątem najnowszych poprawek systemu operacyjnego i składników systemu. Dzięki monitorowaniu podatności i źródeł informacji o wykorzystaniu możliwe będzie uzyskanie bardziej aktualnych informacji. Te dodatkowe badania mogą zaowocować możliwością określenia i wdrożenia tymczasowego rozwiązania do czasu, gdy sprzedawca zapewni trwałą poprawkę. Opracowanie i wydanie poprawki może zająć sprzedawcom tygodnie i miesiące. W niektórych przypadkach poprawki innych firm będą dostępne dla niełatanych, aktywnie wykorzystywanych luk w zabezpieczeniach. Chociaż korzystanie z nich jest opcją, jest niewskazane ze względu na brak możliwości zweryfikowaia integralności i bezpieczeństwo poprawki.

Aktualizacje wzorów.

Zagrożenia ewoluują do woli. Automatyczne aktualizacje zapewniają najmniejszą różnicę w narażeniu na sygnatury złośliwego oprogramowania oparte na wzorcach. Jednak ślepe zaufanie do tych

aktualizacji w środowisku produkcyjnym może mieć niekorzystne skutki. Aby uniknąć problemów, przed wdrożeniem pełnej ochrony należy ustanowić procedurę, która włącza podpisy informacyjne w trybie tylko do monitorowania, aby upewnić się, że nie ma żadnych niepożądanych skutków. Jeśli automatyczne aktualizacje nie są realną opcją, testowanie wymaga środowiska laboratoryjnego lub użycia systemów niekrytycznych w celu sprawdzenia nowych wzorców / sygnatur.

Rejestrowanie i alerty.

Niezależnie od tego, czy pozostają lokalne, czy są przenoszone do scentralizowanego systemu zarządzania, dzienniki zajmują dużą ilość miejsca na dysku, a jeśli nie są przeglądane, nie warto ich przechowywać. Musi istnieć proces przeglądu dziennika. Zamiast próbować określić anomalie na podstawie całego zestawu dzienników, pomocne jest usunięcie znanego ruchu w celu ujawnienia nieznanego i potencjalnie złośliwego. Na przykład, jeśli spodziewasz się wychodzącego ruchu SMTP tylko z jednej sieci, możesz odfiltrować te znane elementy i łatwiej sprawdzić, czy inne nieautoryzowane hosty lub sieci pochodzą z ruchu SMTP. Organizacje z dużym zasięgiem sieci Web będą generować dużą liczbę zdarzeń związanych z HTTP / HTTPS, ponieważ każde nowe połączenie tworzy wpis dziennika. Dysponując GSD wykonującym inspekcję protokołów i rejestrowanie, istnieje możliwość lepszego zrozumienia, czy pakiety są oczekiwane, czy złośliwe. Jeśli istnieją inne systemy śledzące i / lub korelujące te połączenia, przydatne może być wyłączenie logowania na wybranych regułach GSD, aby zmniejszyć nadmiar dzienników, których nie trzeba przeglądać. System zarządzania incydentami i zdarzeniami bezpieczeństwa (SIEM) zapewnia dodatkową metodę zbierania, agregacji i konsolidacji logów z wielu typów urządzeń. SIEM wykorzystuje bazowe i konfigurowalne reguły do skorelowania dzienników i zapewnienia alertów opartych na incydentach w czasie rzeczywistym. Alerty są uzupełnieniem mechanizmu logowania i zwykle od niego zależą. Po wygenerowaniu przez zaporę ogniową lub GSD wpisu w dzienniku administrator może skonfigurować opcje ostrzegania, gdy istnieją określone warunki dziennika lub zmiany progów. Na przykład administrator może skonfigurować alert, aby wysyłał powiadomienie, jeśli stan wewnętrznego procesu systemowego ulegnie zmianie. Dzięki starannemu określeniu progów ostrzegania i metod powiadamiania istnieje mniej możliwości obciążania administratora (-ów) uciążliwymi alertami.

Bezpieczna konfiguracja podstawowa.

Kolejnym kluczowym krokiem do ochrony urządzeń zabezpieczających sieć jest utworzenie bezpiecznej konfiguracji podstawowej. W niektórych przypadkach dostawca GSD dostarcza wzmocnioną i / lub zastrzeżoną wersję systemu operacyjnego. Nie powinno to oznaczać „zielonego światła", że urządzenie jest bezpieczne i gotowe do produkcji. Stanowi to raczej jeszcze więcej powodów, aby poświęcić trochę czasu na dokładną ocenę stanu bezpieczeństwa urządzenia. Po ustawieniu bezpiecznej konfiguracji staje się ona konfiguracją podstawową dla pozostałych systemów. Zapewnia to standardową konfigurację pomagającą zapewnić, że każde urządzenie działa i zabezpiecza w ten sam sposób. Powinien również istnieć proces zapewniający integralność bezpiecznej konfiguracji, a także weryfikujący i testujący, gdy pojawią się ważne aktualizacje.

Konfiguracje domyślne.

Domyślne konfiguracje systemu i zasad są bardzo różne; niektórzy niejawnie zaprzeczają, podczas gdy inni mogą domyślnie zezwalać. W żadnym przypadku żadne urządzenie zabezpieczające sieć nie powinno być wdrażane do produkcji z domyślną konfiguracją. Upewnij się, że określisz, czy urządzenie zabezpieczające sieć uległo awarii w niezabezpieczonej lub bezpiecznej pozycji. Urządzenia wbudowane mogą zawieść niezabezpieczone, próbując utrzymać przepływ ruchu w przypadku awarii. W zależności od sieci może to być optymalna odpowiedź lub nie. Mimo, że potencjalnie uciążliwa,

niezabezpieczona postawa w przypadku awarii zmniejsza prawdopodobieństwo niezauważonego przejścia anomalnego lub złośliwego ruchu.

Zasady dorozumiane.

Domniemane reguły są niezależne od konfiguracji domyślnej, ale stanowią jej część. Urządzenie zabezpieczające sieć będzie przetwarzać niejawne reguły, zanim pakiety dotrą do reguł zasad. Domniemane reguły mogą pozwolić GSD na przetwarzanie określonego i znanego ruchu administracyjnego bez używania cykli przetwarzania do przechodzenia przez całą bazę reguł. Konieczne jest ustalenie, czy te zasady istnieją, a także czy pasują do pożądanej pozycji bezpieczeństwa. Jeśli nie, wyłącz lub zmodyfikuj dorozumiane reguły, aby dostosować je do określonych potrzeb w zakresie ochrony.

Utwardzaj urządzenie.

Ochrona urządzenia zabezpieczającego sieć jest krytyczną częścią bezpieczeństwa całej infrastruktury. Dwa najczęstsze sposoby ograniczania tych zagrożeń to konsola administracyjna i walidacja przy użyciu oceny podatności. Konsola zarządzania lub konsola systemowa może dostarczać informacji, takich jak domyślne porty nasłuchujące, uruchomione usługi i tym podobne. Jeśli usługa nie jest krytyczna dla funkcjonowania zapory, wyłącz ją, aby usunąć wszelkie zagrożenie, że stanie się wektorem zagrożenia. Nawet przy wyłączonej usłudze upewnij się, że nadal aplikujesz poprawki do tych usług. Tylko określone hosty administracyjne powinny mieć bezpośredni dostęp do systemu. Podobnie jak w przypadku zasad GSD, warto sprawdzić, czy zmiany konfiguracji faktycznie zwiększają bezpieczeństwo urządzenia. Przeprowadzając ocenę podatności, możesz określić, czy nieoczekiwane usługi są nadal dostępne, czy też istnieją dodatkowe luki.

Odzyskiwanie po katastrofie.

Wpływ awarii GSD może wahać się od uciążliwości do zdarzenia krytycznego, w zależności od wdrożenia, konieczności i planowania odtwarzania po awarii. Ponieważ systemy te stanowią część szkieletu infrastruktury bezpieczeństwa, konieczne jest zapewnienie ciągłego, chronionego dostępu do sieci.

Awaria / wysoka dostępność.

Architektury o wysokiej dostępności (HA) są niezbędne w sytuacjach, w których niezawodny dostęp jest konieczny. Wdrożenie HA będzie zazwyczaj miało parę Aktywny / Gotowy; gdzie aktywny członek przetwarza aktywne pakiety, a rezerwowy członek jest gotowy do przejęcia w przypadku awarii aktywnego członka. Jeśli członek będący w stanie gotowości nieustannie synchronizuje informacje o połączeniu z aktywnym członkiem, utrata połączenia będzie niewielka lub żadna, jeśli aktywny członek ulegnie awarii, ponieważ stan gotowości stałby się wtedy aktywny i miałby już informacje o połączeniu umożliwiające dalsze przetwarzanie bieżących sesji i obsługi nowych sesji.

Równoważenie obciążenia.

Rozłożenie obciążenia na wiele systemów to kolejny sposób na zmniejszenie narażenia na dostępność. Jeśli obciążenie rozkłada się równomiernie między dwoma lub więcej systemami, awaria jednego nie eliminuje całego dostępu. Jedynym zastrzeżeniem jest to, że moduł równoważenia obciążenia musi nadal kierować każde połączenie do tego samego systemu zaplecza, aby zachować informacje o połączeniu. W przeciwnym razie load balancer może kierować ruch do innego systemu, który nie wie o nawiązanym połączeniu (np. Routing asymetryczny).

Przywracania kopii zapasowej.

Funkcja tworzenia kopii zapasowych i przywracania jest najbardziej podstawową metodą odzyskiwania po awarii. Jeśli system ulegnie awarii lub przejdzie kompromis, musi istnieć sposób na odzyskanie systemu w skuteczny sposób. Posiadając niezawodny proces tworzenia kopii zapasowych, przywrócenie konfiguracji urządzenia w przypadku awarii staje się łatwiejsze. W zależności od dostawcy kopie zapasowe mogą składać się z pliku tekstowego lub czegoś bardziej złożonego, takiego jak plik GZIP zawierający kluczowe informacje o konfiguracji. Proces tworzenia kopii zapasowych musi obejmować metodę przenoszenia kopii zapasowej do innego systemu, aby wyeliminować pojedynczy punkt awarii. Proces przywracania może obejmować przywracanie systemu operacyjnego i / lub konfiguracji urządzenia zabezpieczającego. Może to być tak proste, jak przesłanie pliku kopii zapasowej lub może wymagać połączenia poza pasmem, aby wykonać wstępne prace przed przesłaniem zachowanej konfiguracji.

OCENA URZĄDZENIA BEZPIECZEŃSTWA SIECIOWEGO.

Wraz z ewolucją zagrożeń cyfrowych, muszą też zmieniać się urządzenia zabezpieczające sieć. Koszty łączności internetowej nadal spadają, podobnie jak zdolność wykrywania złożonych zagrożeń. Błędem jest myślenie, że obecne systemy i infrastruktura bezpieczeństwa będą opłacalne przez dłuższy czas. Zasadniczo infrastruktura jest stale poddawana przeglądowi. Jednym z kluczowych momentów na powrót do tych pozycji jest czas wymiany urządzeń zabezpieczających. Skuteczne bezpieczeństwo znajduje się na przecięciu ochrony / funkcjonalności, użyteczności i kosztów. Każda sytuacja wiąże się z wyjątkowymi wyzwaniami i możliwościami - celem jest opracowanie najlepszego rozwiązania zabezpieczającego, które sprosta bieżącym wymaganiom organizacji w zakresie ryzyka. Poniższe sekcje przedstawiają ramy do oceny urządzeń zabezpieczających sieć, które są aktualnie używane lub podczas żądania informacji (RFI). Należy pamiętać, że ta sekcja dotyczy procesu w całym cyklu życia architektury GSD, zamiast przedstawiać szczegółowe wytyczne dotyczące możliwości inspekcji bezpieczeństwa. Te wytyczne stanowią dobrą podstawę do przemyślanej analizy wymagań specyficznych dla miejsca.

Aktualne ograniczenia infrastruktury.

Z technicznego punktu widzenia może być technicznie możliwe zastąpienie istniejącej zapory ogniowej GSD jeden za jeden, ale ważne jest, aby przejrzeć obecną infrastrukturę, aby zapewnić maksymalną skuteczność nowego urządzenia (urządzeń). * Czy obecne urządzenia zabezpieczające sieć minęły lata?

* Obejmuje to urządzenia, które nie są objęte gwarancją, nie są już obsługiwane przez sprzedawcę i nie mogą spełniać aktualnych wymagań.

* Czy architektura z dostępem do Internetu ogranicza opcje wdrażania GSD?

* Posiadanie tylko kilku publicznie rutowalnych adresów IP może ograniczyć liczbę zewnętrznych stref usług bez szerokiego stosowania NAT.

* Umieszczenie GSD w dozwolonej ścieżce całego zaszyfrowanego ruchu może sprawić, że GSD stanie się bardziej filtrem pakietów niż rozszerzalne rozwiązanie bezpieczeństwa.

Nowe wymagania dotyczące infrastruktury.

Dynamika sieci i infrastruktury bezpieczeństwa nieustannie się zmienia. Trendy gwałtownie wzrastającego wykorzystania przepustowości lub zwiększonej zależności od szyfrowanej komunikacji są powszechne. Perspektywa dodania możliwości GSD ma ogromny wpływ na te decyzje.

* Czy są nowe wymagania dotyczące zwiększonej przepustowości, szyfrowania lub wymuszania warstwy aplikacji?

* Określenie nowych wymagań obejmuje obserwowany lub przewidywany / prognozowany wzrost.

* Czy nadmiarowość dostępu do Internetu staje się koniecznością?

* Ważne jest, aby wziąć pod uwagę GSD z wbudowanymi funkcjami redundancji, takimi jak aktywne / pasywne przełączanie awaryjne lub klastrowanie.

* Czy Twoja infrastruktura jest w stanie obsłużyć różnych przewoźników i / lub trasy do Internetu?

Wydajność

Przestarzałe technologie nadal prześladują organizacje, które próbują się rozwijać, aby sprostać wymaganiom wewnętrznym i zewnętrznym.

* Czy istniejące urządzenie ma nadmiar mocy na przyszłe potrzeby?

* Urządzenia zabezpieczające działające przy wysokim wykorzystaniu procesora i / lub pamięci są dobrymi wskaźnikami, że system osiągnął lub osiągnął maksymalny próg wydajności.

* Bez dodatkowej mocy obliczeniowej niewielki wzrost ruchu w sieci lub włączenie nowej funkcji może sparaliżować i tak już pozbawione zasobów urządzenie.

Przepustowość

Potrzeba przepustowości jest nieustająca. Przepustowość 10 Gigabit nie jest już wystarczająca w rdzeniu, ponieważ cena i dostępność 40 i 100 Gigabit są już coraz bardziej dostępne. Standard 802.11ac jest gotowy do przyćmienia ustanowionego standardu bezprzewodowego 802.11n i oferuje deklarowane prędkości gigabitowe na sekundę (lub większe), co prowadzi organizacje do kwestionowania korzystania z łączności przewodowej. Organizacje powinny przyjąć realistyczne podejście, zanim zapłacą za rozwiązania o większej przepustowości.

* Czy urządzenie spełnia wymagania dotyczące przepustowości?

* GSD musi być w stanie wytrzymać niezbędne szczytowe obciążenia ruchem bez przerw lub degradacji usług.

* Czy zagregowane interfejsy sieciowe są obsługiwane w celu obsługi niewielkiej zwiększonej przepustowości zamiast płacenia za interfejsy o większej szybkości (np. Wiele interfejsów Gig w porównaniu z 1 × 10 Gig)?

* Czy urządzenie ma nadmierną pojemność na przyszłe potrzeby?

* Urządzenia modułowe są w stanie zwiększyć pamięć, dodać interfejsy sieciowe lub zwiększyć przepustowość poprzez dodanie lub wymianę modułu sprzętowego.

* Szczyty ruchu sieciowego są nieuniknione. Posiadanie dodatkowej przepustowości dla istniejących segmentów sieci GSD zmniejszy wpływ takich sytuacji.

Implikacje dodatkowych funkcji.

Wielu dostawców zachwala przepustowość przy (lub bliskich) prędkościach drutu. Jednak statystyki te niekoniecznie odzwierciedlają rzeczywistość, ponieważ standardowe testy przepustowości zawsze uwzględniają różne rozmiary pakietów i mieszaniny protokołów. W rzeczywistości typy i rozmiary pakietów stale się zmieniają; pamiętaj, aby przejrzeć oświadczenia dostawców za pośrednictwem niezależnej organizacji testującej i, jeśli to możliwe, testów wewnętrznych.

* Jaki wpływ na wydajność ma aktywacja dodatkowych funkcji bezpieczeństwa?

* Im większa liczba dodatkowych funkcji - zwykle skutkujących bardziej szczegółową kontrolą ładunku - tym większy negatywny wpływ na moc obliczeniową urządzenia i przepustowość.

* Jeśli wymagane jest szyfrowanie, przyspieszenie sprzętowe, jeśli jest dostępne, zmniejszy w znacznym stopniu ten wpływ na wydajność.

* Pamiętaj, aby ocenić dokumentację dostawcy i niezależną, pokazującą zmierzoną wydajność w odniesieniu do różnych przepływów ruchu, takich jak IMIX (Internet Mix) i EMIX (Enterprise Mix).

* Jaki poziom dodatkowego obciążenia administracyjnego stworzą funkcje?

* Konsolidacja zarządzania wieloma funkcjami bezpieczeństwa niekoniecznie ułatwia zarządzanie nimi. To również zwiększa złożoność w zależności od sposobu integracji każdego podsystemu

Zarządzanie

GSD zazwyczaj wymagają znacznego planowania, konfiguracji, monitorowania i konserwacji. Posiadanie solidnej platformy zarządzania w rozproszonych środowiskach GSD ma zasadnicze znaczenie dla powodzenia wdrożenia.

* Czy obecne środowisko ma potrzebne lub wymagane funkcje zarządzania?

* Samoocena obecnego środowiska zarządzania jest dość łatwa, ponieważ istnieją już ustalone upodobania, niechęci, miłe osoby, rzeczy niezbędne i których nie można mieć.

* Czy istnieje potrzeba / potrzeba zarządzania rozproszonego lub scentralizowanego?

* Należy wziąć pod uwagę rozmiar i typ rozmieszczenia GSD. Prawdopodobnie nie ma sensu stosowanie rozbudowanej platformy do zarządzania kilkoma urządzeniami. W większych środowiskach rozproszonych geograficznie centralne sterowanie wszystkimi urządzeniami jest niezbędne do wydajnego i skutecznego dowodzenia i kontroli.

* Czy potrzebne są nadmiarowe systemy zarządzania?

* Nadmiarowe systemy zarządzania zapewniają kontrolę administracyjną i logowanie urządzeń GSD w przypadku awarii. Pamiętaj, aby przejrzeć opcje nadmiarowości systemów zarządzania, aby upewnić się, że system pomocniczy ma parzystość funkcjonalną.

* Czy możliwość zarządzania systemem zarówno ze scentralizowanej konsoli zarządzającej i / lub bezpośrednio z urządzenia jest koniecznością?

* Niektóre typy GSD umożliwiają wprowadzanie zmian systemowych i zasad bezpośrednio z urządzenia. Ta funkcja może być przydatna podczas testowania lub rozwiązywania problemów, ale może powodować zamieszanie lub błędną konfigurację, jeśli nie zostanie odpowiednio zrozumiana i zarządzana.

* Czy szyfrowanie jest wymagane do ochrony funkcji zarządzania, zasad i rejestrowania?

* Potrzeba zaszyfrowania poufnych informacji jest ważną kwestią przy przesyłaniu funkcji zarządzania GSD i logowania. W przypadku przesłania zwykłego tekstu ktoś może monitorować tę komunikację i uzyskać istotne informacje na temat architektury bezpieczeństwa sieci.

* Czy szczegółowy mechanizm raportowania jest koniecznością?

* Większość systemów rejestrowania zapewnia możliwość filtrowania danych, ale może być przydatne wykonanie bardziej szczegółowych raportów. Niektóre przykładowe raporty obejmują wartości procentowe bazowych trafień reguł (np. Które reguły otrzymują najwyższy procent trafień) lub statystyki wykorzystania ruchu (np. Procent wykorzystania według protokołu, segmentu sieci, hosta i / lub użytkownika).

* Jaki poziom szczegółowości jest wymagany w przypadku uprawnień do zarządzania?

* W przypadku kilku administratorów może to nie być tak istotne, ale większe wdrożenia mogą mieć rozproszonych administratorów. System zarządzania GSD musi zapewniać bezpieczeństwo oparte na rolach z możliwością ograniczenia dostępu do niektórych zadań, obszarów i / lub dzienników. Przydatne może być podzielenie systemów i zezwolenie innym zespołom pomocy technicznej na dostęp tylko do wyświetlania w celu rozwiązywania problemów i przeprowadzania audytów.

* Czy wymagane są zarówno GUI, jak i / lub polityka wiersza poleceń lub opcje zarządzania urządzeniem?

* Niektóre marki GSD mają opcję konfigurowania urządzeń przy użyciu bardziej tradycyjnego interfejsu wiersza poleceń i mogą być przydatne do szybkiego rozwiązywania problemów i zmian skryptowych. Środowisko graficzne typu „przeciągnij i upuść" wykorzystuje centralne systemy zarządzania do łatwego tworzenia, zmieniania i przeglądania zasad i dzienników. Jeśli obie opcje są dostępne, upewnij się, że mają one parzystość funkcji.

Rejestrowanie i alerty

Chociaż głównym obowiązkiem GSD jest blokowanie złośliwego ruchu, rejestrowanie i ostrzeganie odgrywają kluczową rolę w ogólnym stanie bezpieczeństwa. Rejestrowanie jest niezbędne do badania incydentów, przeglądania trendów, a nawet może być wymogiem regulacyjnym.

* Jak chcesz mieć możliwość filtrowania dzienników?

* Zbieranie, wyszukiwanie i przeglądanie dzienników w formacie tekstowym ma zalety, w tym konsolidację i tworzenie skryptów do przeglądania dzienników. Dzienniki tekstowe wymagają skryptów do analizowania dzienników, ale mają tę zaletę, że mogą używać złożonych zapytań i analizować dzienniki w praktycznie każdym systemie.

* Graficzne interfejsy użytkownika (GUI) zapewniają możliwość filtrowania dzienników na podstawie jednego lub większej liczby kryteriów, ale są słabe podczas wykonywania złożonych lub rekurencyjnych zapytań. Graficzny interfejs użytkownika zwiększa estetykę dzienników i może ułatwić przeglądanie, grupując lub filtrując różne typy zdarzeń, a także dodając kolory i / lub grafiki, które pomagają szybciej przyciągnąć uwagę. Chociaż jest użyteczny, GUI może ładować się wolniej i może ograniczać możliwość tworzenia złożonych zapytań.

* Czy chcesz, aby dzienniki były kompresowane?

* Nawet przy dobrze utrzymanych standardach rejestrowania i procesach pielęgnacji sama ilość logów GSD może być przytłaczająca. Dzienniki tekstowe zazwyczaj zapewniają wysoki współczynnik kompresji i łatwą archiwizację. Niektóre z zastrzeżonych formatów mogą automatycznie zapewniać pewną kompresję, ale mogą nie być w stanie dopasować się do formatów niezastrzeżonych.

* Jak chcesz przechowywać logi?

* Opcje rejestrowania GSD obejmują przechowywanie na urządzeniu lokalnym, na zintegrowanej platformie logowania i zarządzania lub na oddzielnym urządzeniu magazynującym. Lokalna pamięć

masowa stwarza ryzyko utraty danych w przypadku awarii GSD lub potencjalny wpływ na system, jeśli dzienniki zapełniają lokalną pamięć. Wysyłanie dzienników do innych systemów zwiększy ruch w sieci, ale zapewnia to łatwiejsze zarządzanie dziennikami przez cały cykl życia informacji.

* Jakiego rodzaju i szczegółowości alertów potrzebujesz?

* Alerty pomagają ożywić informacje bez konieczności oglądania dzienników w każdej minucie dnia. Możliwe jest utworzenie alertów e-mail lub SMS, gdy wystąpi zdarzenie, które przekroczy skonfigurowany próg (np. Przepustowość sieci GSD przekracza 85% maksymalnej możliwej lub host próbuje zaatakować GSD).

* Możliwe może być opracowanie szczegółowych warunków ostrzegania (np. Zależności kryteriów) w celu zminimalizowania błędnych alertów.

* Czy masz prawne i / lub regulacyjne wymagania dotyczące prowadzenia dzienników przez określony czas?

* Wymagania wewnętrzne i / lub regulacyjne mogą wymagać przechowywania tych danych od miesięcy do wielu lat

Audyt

Rejestry audytów zawierają informacje o tym, jakie zmiany wystąpiły, kiedy, przez kogo i tak dalej. Posiadanie zintegrowanej ścieżki audytu zmian środowiska GSD może być nieocenione podczas incydentu.

* Czy chcesz mieć możliwość audytu zmian urządzeń?

* Zmiany w samym urządzeniu nie są tak częste, jak zmiany w zasadach. Możliwość zbierania informacji o tych zmianach może pomóc w wykryciu niestabilności systemu, przypadkowej błędnej konfiguracji i / lub złośliwych zamiarów.

* Czy chcesz mieć możliwość inspekcji zmian zasad?

* Zasady GSD zmieniają się szybko, gdy rozwijają się nowe wymagania dotyczące dostępu, pojawiają się nowe możliwości lub wymagania oraz stale zmieniający się krajobraz zagrożeń. Ścieżki audytu polityki pomagają rozwiązywać błędy i dostarczają archiwalnych informacji o tym, jakie zmiany zaszły i kiedy.

* Jaki poziom szczegółowej kontroli jest wymagany?

* Dane takie jak data, godzina, rodzaj zmiany, do jakiego systemu (-ów) i od jakiego administratora są cenne informacje. Zwiększenie szczegółowości inspekcji może zwiększyć ogólną objętość dziennika i narzut przetwarzania.

* Czy dzienniki audytu powinny być niezależne od dzienników zdarzeń zapory?

* Posiadanie systemu rejestrowania, który automatycznie oddziela dzienniki audytu od innych dzienników zdarzeń, ułatwia przeglądanie i wyszukiwanie. Daje to również możliwość tworzenia bardziej szczegółowych poziomów uprawnień (np. Kto może zobaczyć, jakiego rodzaju dzienniki).

Odzyskiwanie po awarii

Dzięki GSD zapewniającym skonsolidowane funkcje bezpieczeństwa, włączenie opcji odzyskiwania po awarii (DR) do środowiska GSD pomaga zapewnić, że nie stanie się ono pojedynczym punktem awarii dla całej organizacji.

* Jakie są Twoje wymagania dotyczące odzyskiwania po awarii?

* Jak wspomniano wcześniej, różne typy nadmiarowości pomagają w scenariuszach DR. Konfiguracje wysokiej dostępności, takie jak aktywne / pasywne przełączanie awaryjne i klastrowanie, mogą pomóc w zwiększeniu ogólnej dostępności.

* Czy urządzenie ma łatwe w użyciu mechanizmy tworzenia kopii zapasowych i przywracania?

* Mechanizm tworzenia kopii zapasowych powinien zapewniać prosty interfejs do wykonywania kopii zapasowych i przywracania, a także przenoszenia ich z urządzenia lokalnego w celu przechowywania i archiwizacji.

* Czy chcesz mieć możliwość automatycznego przywracania?

* Niektóre GSD mają możliwość automatycznego lub półautomatycznego przywracania za pomocą skryptów lub poprzez konfiguracje wysyłane z systemu zarządzania.

* Czy system powinien zawieść bezpieczny lub niepewny?

* Ważne jest, aby określić, czy przewaga czasu pracy systemu niezabezpieczonego przed awarią przeważa nad ryzykiem przejścia ruchu sieciowego bez kontroli lub przestojów związanych z systemem odpornym na awarie.

* Czy potrzebujesz dostępu poza pasmem?

* Posiadanie rozwiązania dostępu pozapasmowego, takiego jak bezpośrednie połączenie szeregowe i / lub rozwiązanie dial-in, może zapewnić możliwość monitorowania i / lub zmiany systemu podczas awarii sieci.

Użyteczność

Posiadanie środowiska zarządzania, które ma wszystkie możliwe do wyobrażenia funkcje, jest bezwartościowe, jeśli jest zbyt złożone i zawiłe w obsłudze i utrzymaniu.

* Czy konsola zarządzania jest intuicyjna?

* Konsola zarządzania powinna mieć spójny i prosty interfejs do zarządzania urządzeniami i zasadami. Im bardziej intuicyjny interfejs, tym mniej czasu administratorzy będą musieli poświęcić na zastanawianie się, jak wykonywać proste zadania lub rozwiązywać problemy.

* Czy podstawowe funkcje są łatwe do wykonania?

* Interfejs powinien ułatwiać śledzenie i edytowanie zasad, a także przeglądanie i filtrowanie dzienników.

Krzywa uczenia się

Wybierając dostawcę GSD z intuicyjnym interfejsem i funkcjonalnością, powinno być dużo łatwiej poznać środowisko.

* Czy wymagane jest szkolenie, aby nauczyć się nowego urządzenia (urządzeń) i platformy zarządzania?

* Nawet z najlepszym interfejsem i funkcjami może być konieczne przeszkolenie administratora (ów) w zakresie efektywnego korzystania z systemu. Skontaktuj się z dostawcą, aby dowiedzieć się, jakie szkolenia (od podstawowego do zaawansowanego) są dostępne i za jaką cenę. Jeśli to możliwe, określ skuteczność instruktora (-ów) poprzez skierowania.

* Jeśli niektóre funkcje zabezpieczeń są nowe w organizacji, spodziewaj się bardziej stromej początkowej i zwiększonej krzywej uczenia się ze względu na szerokość i głębokość każdego dodatkowego środka ochrony.

* Jak dostawca podchodzi do architektury bezpieczeństwa?

* Każdy dostawca GSD ma trochę inny pogląd i implementację funkcji bezpieczeństwa. Niektóre koncentrują się głównie na dopuszczaniu lub odrzucaniu ruchu, podczas gdy inne traktują ruch sieciowy jako przepływy między strefami. Przejście od jednego typu dostawcy do innego może być mylące i może spowolnić lub zmylić konwersję.

Cechy

Chociaż platforma GSD może być w stanie zapewnić pojedyncze źródło zabezpieczeń sieci, należy pamiętać, że spełnienie potrzeb i postawy organizacji w zakresie bezpieczeństwa może nie być opłacalne ani efektywne pod względem zasobów.

* Szukasz urządzenia, które będzie rozwiązaniem typu „wszystko w jednym”?

* Możliwość zapewnienia pojedynczej platformy bezpieczeństwa rozwiązania ma zalety, ale każda dodatkowa funkcja ma wpływ na wydajność i dostępność, a nieprawidłowo wdrożona zwiększa potencjalne problemy.

* Jakie funkcje ma mieć GSD?

* Typowe funkcje UTM mogą obejmować zaporę ogniową, IPS, VPN, ochronę przed złośliwym oprogramowaniem, antyspam, DLP i Quality of Service (QoS).

* Typowe funkcje NGFW obejmują niezależną od portu identyfikację aplikacji i egzekwowanie podfunkcji określonego protokołu.

* Czy platforma obsługuje pełne egzekwowanie protokołu IPv6 we wszystkich funkcjach bezpieczeństwa?

Cena

Upewnij się, że rozumiesz wpływ kosztów całej infrastruktury GSD na cały okres jej użytkowania.

* Jaki będzie całkowity koszt posiadania (TCO) aktualizacji lub wymiany?

* Obszary do rozważenia obejmują: cenę zakupu sprzętu; cena za żądane funkcje bezpieczeństwa (dodatkowe funkcje, jeśli zostaną dodane później, zwiększą całkowite koszty i mogą wymagać nowego sprzętu); infrastruktura zarządzania (sprzęt i oprogramowanie); opłaty za utrzymanie sprzętu i oprogramowania; koszty szkolenia; umowa wsparcia bezpośredniego lub strony trzeciej; potencjalny przestój konwersji; i krzywej uczenia się.

Koszt początkowy

* Ile będzie kosztować nowy sprzęt GSD?

* Obejmuje cenę GSD, kart rozszerzeń i urządzeń zarządzających.

* Urządzenie może być bardziej opłacalną alternatywą długoterminową, jeśli istnieje wiele opcji wdrożenia, ponieważ sprzedawca ponosi wyłączną odpowiedzialność za problemy.

* Ile dodatkowo będzie kosztowała wysyłka?

* W przypadku wdrożenia rozproszonego mogą wystąpić dodatkowe koszty wysyłki i taryfy związane z dostawą sprzętu do lokalizacji międzynarodowych.

* Ile będzie kosztować zakup funkcji, których potrzebuję?

* Zależy to w dużym stopniu od GSD. Niektóre GSD są dostarczane ze wszystkim po wyjęciu z pudełka, podczas gdy inne zapewniają podstawowe funkcje, w tym zaporę ogniową, VPN i podstawową kontrolę protokołów, ale pobierają dodatkową opłatę za korzystanie z pełnej funkcjonalności istniejących elementów i / lub dodawanie nowych funkcji.

* Ile trzeba zainwestować w szkolenie, aby nauczyć się nowego rozwiązania?

* Szkolenie często obejmuje udział w kursach poza siedzibą firmy (co może wymagać dodatkowych kosztów podróży). W niektórych przypadkach bardziej opłacalne może być zatrudnienie trenera na miejscu w celu zapewnienia bardziej dostosowanego programu szkoleniowego. Metodologia szkolenia trenera może być opcją pozwalającą zaoszczędzić pieniądze, w zależności od wielkości zespołu i finansowania.

Koszty bieżące

* Ile kosztuje roczna konserwacja sprzętu i / lub oprogramowania?

* Umowa serwisowa może podlegać negocjacjom na podstawie długości okresu i kosztów (potencjalnie na podstawie procentu zakupu).

* Jakiego poziomu usług potrzebujesz?

* Dostawcy GSD zapewniają różne poziomy usług w zależności od czasu reakcji, możliwości eskalacji i dostępu do dodatkowych informacji. Zgodnie z tym, im wyższy poziom usług, tym więcej będzie to kosztować.

* Czy dostawca może wspierać Cię w każdej lokalizacji?

* W razie potrzeby poważne problemy mogą wymagać przybycia dostawcy lub partnera dostawcy na miejsce naprawy. Jeśli to możliwe, określ koszt (czas i dojazd) przed skorzystaniem z tego typu usługi.

* W przypadku wdrożeń międzynarodowych należy zapoznać się ze zdolnością dostawcy do zapewnienia ogólnej naprawy gwarancyjnej i / lub serwisu na miejscu w tych lokalizacjach.

* Czy istnieje zapotrzebowanie na zapasowe urządzenie na miejscu?

* Jeśli plan odzyskiwania po awarii wymaga szybkiego przywrócenia, pomocna może być posiadanie części zapasowej na miejscu. Wadą posiadania zapasowej (a nie nadmiarowej pary) jest to, że najprawdopodobniej stanie się ona bezczynnym zasobem. Pamiętaj, aby porównać to z kosztem umowy serwisowej wyższego poziomu lub lokalną dostępnością części zamiennych.

* Czy potrzebujesz dodatkowego czasu na konsultacje / wsparcie?

* Dostawcy i partnerzy mogą zapewniać bloki czasowe, w których dedykowane zasoby mogą przyjść na miejsce w celu uzyskania dodatkowego wsparcia, planowania i recenzji platformy.

Uwagi dotyczące dostawcy

Możliwość zaufania, że produkt dostawcy będzie chronić organizację, ma kluczowe znaczenie. Upewnij się, że czujesz się komfortowo w każdym aspekcie produktu i usługi, zanim zdejmiesz kontrolę nad bezpieczeństwem sieci. Oprócz uzyskania wymaganych funkcji dostawca dostarczający rozwiązanie

powinien mieć solidne podstawy bezpieczeństwa, stabilność finansową i odpowiednie zasoby wsparcia.

* Czy ten dostawca spełni obecne i przyszłe potrzeby organizacji?

* To kluczowe pytanie koncentruje się na zdolności dostawcy do zapewnienia wysokiej jakości produktu, wsparcia tego produktu i rozwoju zgodnie z Twoimi potrzebami. Pamiętaj, aby ocenić mapę drogową produktu dostawcy, aby zobaczyć, jak produkt będzie ewoluował (sprzęt, funkcjonalność, koszt itp.) I kiedy aktualnie niedostępne funkcje będą dostępne w produkcie.

* Czy dostawca już obsługuje lub ma doświadczenie z wdrożeniami podobnymi do Twojego?

* Jeśli dostawca ma już klientów z infrastrukturą i potrzebami podobnymi do Twoich, może to dostarczyć dodatkowych pomysłów i / lub informacji, które sprawią, że wdrożenie będzie skuteczniejsze.

Reputacja

Chociaż spory wewnętrzne i opinie na temat najlepszych platform bezpieczeństwa są liczne, wybrany dostawca powinien być aktywnym członkiem społeczności bezpieczeństwa.

* Czy ten dostawca cieszy się dobrą opinią w społeczności zajmującej się bezpieczeństwem?

* Nie brakuje recenzji produktów i porównań, które pomagają określić, czy produkt lub sprzedawca ma solidną reputację w zakresie jakości i usług. Nie są one ostatecznym arbitrem dobrego produktu, ale stanowią podstawę do dodatkowych badań.

* Czy zapewnią referencje?

* Skontaktuj się ze sprzedawcą, aby sprawdzić, czy inna firma (lub dwie) dostarczy odniesienia do swoich doświadczeń z produktem i usługą.

* Jaka jest historia luk w zabezpieczeniach obecnego i poprzednich systemów?

* Sprawdź podatności i wykorzystaj strony monitorujące, aby określić historię luk.

* Jaki jest średni czas naprawy luk?

* Chociaż optymalny czas na usunięcie luki jest natychmiastowy (lub zapobieżenie temu, zanim to się stanie), sprawdź, ile czasu zajmuje producentom reagowanie na luki i usuwanie ich. Obejmuje to sprawdzenie, czy poprawka rozwiązała problem za pierwszym razem.

* Jaki jest średni czas na poprawienie problemów i / lub luk dotyczących tożsamości aplikacji?

* Złożoność i zmienny charakter protokołów warstwy aplikacji wymaga aktywnego udziału dostawców. Określ proces, ramy czasowe i potencjalne koszty związane z korektą (lub obsługą) potrzeb związanych z tożsamością aplikacji przez dostawcę.

Opcje wsparcia

Ze względu na złożoność i szeroki zakres funkcji, jakie te urządzenia posiadają, wybrani dostawcy muszą mieć solidną infrastrukturę wsparcia, aby rozwiązywać problemy.

* Jakie doświadczenie mają technicy z pierwszej linii i wyższego szczebla?

* Poproś dostawcę o podanie informacji dotyczących szkolenia i doświadczenia na różnych poziomach wsparcia technicznego.

* Czy istnieją różne poziomy wstępnej pomocy telefonicznej?

* Określić, czy wszystkie zgłoszenia do pomocy technicznej są wysyłane za pośrednictwem głównego działu wsparcia / działu obsługi, czy też możliwe jest posiadanie dedykowanego (zwykle współdzielonego przez inne obsługiwane organizacje) zasobu.

* Czy masz możliwość eskalacji na żądanie?

* Ustal, czy możliwa jest natychmiastowa eskalacja problemu (i za jaką cenę), jeśli lokalni administratorzy wykonają standardowe kroki rozwiązywania problemów.

* Czy chcesz pracować z systemami podczas testów beta?

* W zależności od tolerancji na ryzyko bycie partnerem w wersji beta z dostawcą może zapewnić wczesny dostęp do poprawek i ulepszeń.

* Jakie są obecne i poprzednie doświadczenia klientów z jakością i dostępnością pomocy technicznej?

* Ponownie poproś o referencje, aby uzyskać perspektywę świata rzeczywistego.

Zarządzani dostawcy usług bezpieczeństwa

Organizacje mają możliwość przenoszenia różnych poziomów odpowiedzialności za bezpieczeństwo sieci wewnętrznej do dostawcy usług zarządzania zabezpieczeniami (MSSP). Korzystanie z MSSP może być okazją do uzupełnienia przeglądów dzienników poza zmianą, konsolidacji i / lub tworzenia alertów. Ponadto może istnieć możliwość przeniesienia obsługi i kontroli zmian w celu złagodzenia wewnętrznych ograniczeń zasobów i / lub luk w wiedzy. Wybór tego typu usługi wymaga szczegółowego zbadania.

* Jaka jest reputacja / doświadczenie / obciążenie MSSP?

* MSSP powinien mieć wyszkolony i doświadczony personel do obsługi infrastruktury GSD.

* Określić liczbę klientów przypadających na zasób wsparcia i czy inne lokalizacje MSSP mogą kontynuować wsparcie i operacje w przypadku awarii w jednej lokalizacji MSSP.

* Czy można to zrobić bezpiecznie?

* Zapewnienie zgodności MSSP z bezpiecznym przechowywaniem zebranych informacji i dostępem do infrastruktury zarządzania GSD.

* W razie potrzeby, w jaki sposób MSSP będzie postępować zgodnie z kontrolą zmian?

* Określ proces kontroli zmian przed przekazaniem odpowiedzialności operacyjnej. Obejmuje to określanie przeglądów zmian, okien zmian, zatwierdzeń zmian, umów SLA dotyczących czasu ukończenia itp.

* Czy MSSP może spełnić Twoje wymagania SLA?

* Ustal jasne oczekiwania podczas negocjacji kontraktowych przy zawieraniu umów SLA. Im bardziej rygorystyczna umowa SLA, tym większe prawdopodobieństwo wzrostu kosztu. Opracuj wskaźniki, aby ocenić skuteczność MSSP w spełnianiu wymagań SLA.

* Za jaką cenę?

* Koszt prowadzenia działalności z MSSP wzrasta w zależności od liczby usług i / lub urządzeń. Pamiętaj, aby zapoznać się z umową, aby zrozumieć wszystkie potencjalne opłaty lub dodatkowe wymagania, które mogą podnieść koszty po podpisaniu pierwotnej umowy.

UWAGI KOŃCOWE

Wymagania dotyczące bezpieczeństwa sieci stale się zmieniają. Organizacje są pod ciągłą presją, aby sprostać wymaganiom klientów i partnerów biznesowych w zakresie informacji i dostępu. Technologie takie jak urządzenia mobilne i ekstranety nadal zacierają dotychczasową rzeczywistość prawdziwych granic sieci. Zabezpieczenie granic nie jest już tak łatwe, jak zainstalowanie zapory lub wymaganie usług proxy dla połączeń wychodzących. Polegaj na określonej technologii lub zabezpieczeniach gdzie ideologia jest niewystarczająca, aby chronić informacje i systemy stanowiące integralną część sukcesu organizacji. Częstotliwość i prawdziwość ataków zewnętrznych i wewnętrznych wymaga solidniejszego i bardziej elastycznego mechanizmu do zwalczania tych rosnących zagrożeń, a GSD skoczył naprzód, aby zapewnić obecną generację technologii ochrony obwodowej. GSD zachowuje wszystkie poprzednie funkcje oparte na zaporze ogniowej, takie jak kontrola dozwolonych ścieżek, usługi VPN i translacja adresów sieciowych, zapewniając jednocześnie elastyczność integracji dodatkowych usług zaprojektowanych w celu zapewnienia widoczności i ochrony przed wieloma zagrożeniami. Dodanie funkcji ochrony przed złośliwym oprogramowaniem zapewnia nową warstwę ochrony, uwalniając hosty od bycia jedyną lokalizacją zapewniającą pełne usługi wykrywania, zapobiegania i naprawiania. Integracja usług proxy, kontroli aplikacji i treści oraz zapobiegania włamaniom umożliwia wdrożeniom GSD uproszczenie architektury bezpieczeństwa sieci i otwiera nowe możliwości inspekcji i ochrony. Dzisiejsze zagrożenia zapewniają niewielki wgląd w to, jak środki ochrony będą musiały ewoluować, aby sprostać atakom i napastnikom nowej generacji. Aby pozostać realną opcją bezpieczeństwa, dostawcy zabezpieczeń GSD muszą zachować elastyczność. Integracja i wdrażanie nowych środków ochrony będzie musiała być prosta i płynna. Wraz ze wzrostem mocy obliczeniowej zwiększą się również możliwości GSD w zakresie przyjmowania większych obciążeń i złożoności. Podstawowa inspekcja treści umożliwi lepsze zrozumienie i ochronę kontekstu, wartości i przepływów danych. Obsługa i ochrona światowych sieci będzie wymagała zapewnienia pełnego zestawu funkcjonalności GSD dla ruchu IPv6. Bez względu na zagrożenie, bez względu na sieć, żadne urządzenie nie jest srebrną kulą zapewniającą pełne bezpieczeństwo. Każda organizacja musi ocenić wszystkie sposoby ochrony, aby upewnić się, że wdrożone technologie spełniają wymagane funkcje bezpieczeństwa.