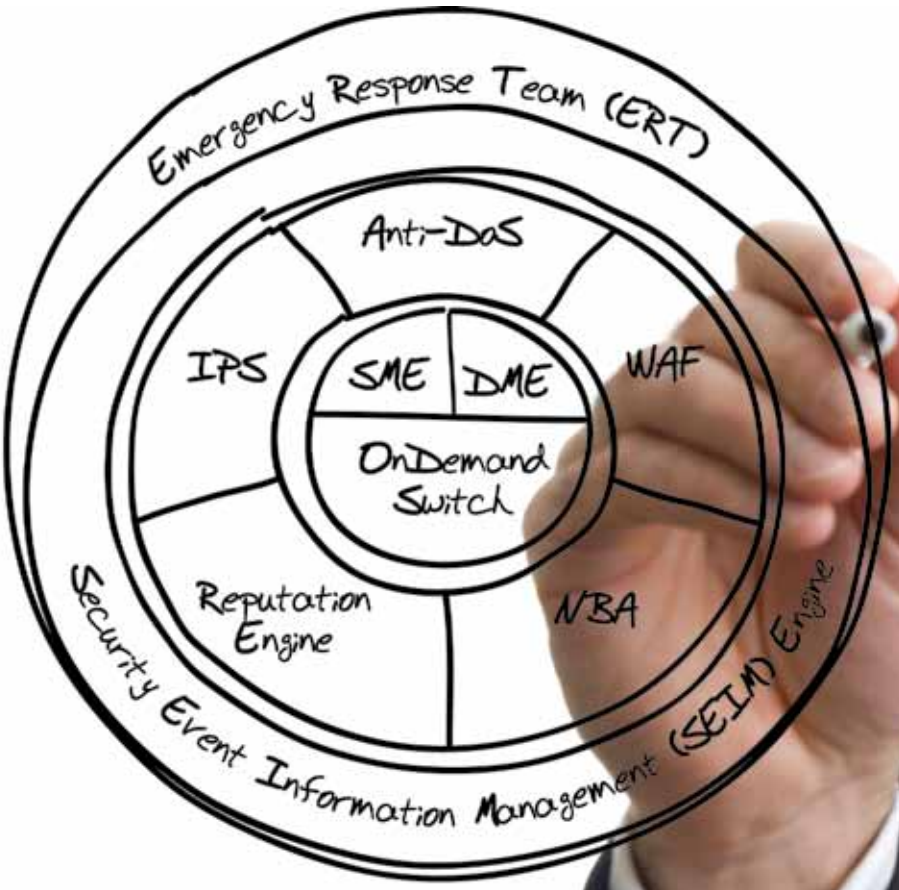
Smart Network. Smart Business.



radware

Rozwiązanie Attack Mitigation System

Rozwiązanie Attack Mitigation System

Chroń swoją działalność online i centra danych przed nowymi zagrożeniami sieciowymi i aplikacji

Nowe zagrożenia stale pojawiające się w sieci wymagają wielu zabezpieczeń, aby zagwarantować bezpieczeństwo firmy

Kierownicy centrów danych i osoby odpowiedzialne za bezpieczeństwo sieci muszą się zmierzyć z coraz większą liczbą zagrożeń o coraz bardziej zróżnicowanym charakterze. Potencjalne niebezpieczeństwa obejmują: awarie sieci, awarie aplikacji, punkty wrażliwe aplikacji, kradzież informacji, złamanie mechanizmów uwierzytelniania, rozpowszechnianie złośliwego oprogramowania, ataki na aplikacje WWW oraz podmiana treści i wyglądu stron WWW.

W ostatnich atakach intruzi posługiwali się nowym technikami, określanymi jako kampanie ataków na wiele punktów wrażliwych. Napastnicy zestawiają sieć typu botnet (lub wskazują swoim fanom, w jaki sposób to zrobić, jak to ma miejsce w przypadku działań grupy Anonymous). Chodzi o to, aby wykonać równocześnie ataki różnych typów, wymierzone w wiele wrażliwych punktów atakowanej infrastruktury informatycznej, jak np. sieci, serwery i warstwy aplikacyjne. Kampanie ataków na wiele punktów wrażliwych mają wyjątkowo niszczące działanie, nawet jeżeli poszczególne kierunki ataków są już dobrze znane (np.: atak UDP flood obciążający przepustowość sieci; atak SYN flood skierowany przeciwko zasobom serwera; atak HTTP Get flood skierowany przeciwko zasobom aplikacji WWW). Atakowany system jest szczególnie zagrożony, ponieważ nawet jeśli tylko jeden z kanałów ataku jest skuteczny – jego rezultat będzie bardzo dotkliwy. Napastnicy wychodzą z założenia, że nawet jeżeli atakowany posiada szereg zabezpieczeń, w ich sieci zewnętrznej istnieje wiele niekontrolowanych punktów, więc któreś z ataków okażą się skuteczne.

Co więcej, standardowe systemy bezpieczeństwa sieci i aplikacji nie są w stanie zapobiegać atakom polegającym na rozprzestrzenianiu złośliwego oprogramowania typu „zero minute" (w momencie ich pierwszego pojawienia się), instalacjom trojanów oraz atakom sieci typu botnet.

W celu zwalczania tej rosnącej liczny zagrożeń osoby odpowiedzialne za zabezpieczenia są zmuszone wdrażać szereg narzędzi do wykrywania i ochrony systemów: systemy zapobiegania penetracji (Intrusion Prevention Systems, IPS), ochronę przed atakami DoS, mechanizmy sieciowej analizy behawioralnej (Network Behavioral Analysis, NBA), narzędzia do oceny reputacji adresów IP oraz zapory Web Application Firewall (WAF).

Attack Mitigation System: zabezpiecz swoją infrastrukturę aplikacyjną przed znanymi i nowymi zagrożeniami sieci i aplikacji w czasie rzeczywistym

Ochrona infrastruktury aplikacyjnej wymaga wdrożenia wielu zabezpieczeń. Attack Mitigation System (AMS) firmy Radware to rozwiązanie służące do łagodzenia ataków na sieci i aplikacje w czasie rzeczywistym, które chroni infrastrukturę aplikacyjną przed awariami sieci i aplikacji, wykorzystaniem słabych punktów aplikacji, rozprzestrzenianiem złośliwego oprogramowania, kradzieżą informacji, atakami na usługi WWW oraz podmianą treści i wyglądu stron WWW.

Rozwiązanie Attack Mitigation System firmy Radware składa się z trzech warstw:

- Warstwa zabezpieczeń – zbiór modułów bezpieczeństwa, obejmujących: **ochronę przed atakami typu Denial-of-service (DoS), mechanizm analizy behawioralnej sieci (Network Behavioral Analysis, NBA), system zapobiegania penetracji (Intrusion Prevention System, IPS), mechanizm Reputation Engine oraz Web Application Firewall (WAF),** które w pełni zabezpieczają sieci, serwery i aplikacje przed znanymi i pojawiającymi się nowymi zagrożeniami bezpieczeństwa sieciowego;

- Zarządzanie zagrożeniami – wbudowany **mechanizm zarządzania informacjami o zdarzeniach z zakresu bezpieczeństwa (Security Event Information Management, SEIM)**, zbierający i analizujący zdarzenia ze wszystkich modułów, który pozwala stworzyć widok stanu gotowości w skali całego przedsiębiorstwa;

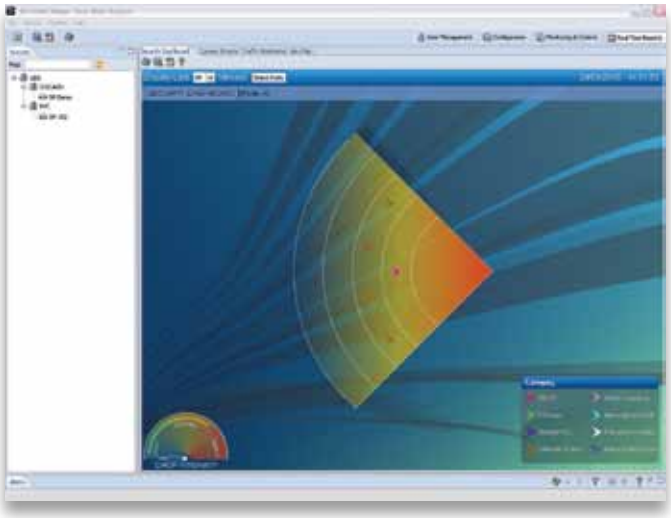
- **Zespół reagowania awaryjnego (Emergency Response Team, ERT)**, składający się z wyspecjalizowanych ekspertów z zakresu bezpieczeństwa, świadczący 24 godziny na dobę i 7 dni w tygodniu błyskawiczne usługi dla klientów, którym grozi atak typu denial-of-service (DoS), w celu przywrócenia sieci i usług do stanu sprawności.

Rys. 1. Rozwiązanie AMS oferuje pełny zestaw modułów zabezpieczeń oraz usług dla firm funkcjonujących w sieci oraz do ochrony centrów danych

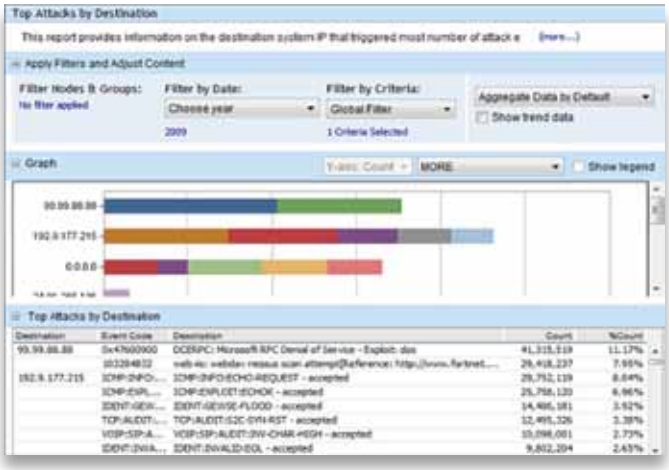
Synergia wielu modułów zabezpieczeń składających się na jeden system umożliwia skuteczniejszą ochronę przeciwko napastnikom, którzy w systematyczny sposób dążą do zniszczenia zasobów biznesowych – zwłaszcza w porównaniu z oddzielnymi, pojedynczymi rozwiązaniami, a jednocześnie oferuje ujednolicone mechanizmy sprawozdawcze i gwarantujące zgodność z wymogami prawnymi.

Wbudowany mechanizm zarządzania informacjami o zdarzeniach z zakresu bezpieczeństwa (SEIM) zapewnia identyfikację, priorytetyzację i reakcję na cyberataki w czasie rzeczywistym.

Wbudowany mechanizm zarządzania informacjami o zdarzeniach z zakresu bezpieczeństwa (Security Event Information Management, SEIM) oferuje widok stanu bezpieczeństwa i zgodności z wymogami w skali całego przedsiębiorstwa z poziomu jednej konsoli. Dane z wielu źródeł są zbierane i konsolidowane do postaci paneli kontrolnych i sprawozdań. Widoki te dają bogate, chociaż proste w obsłudze możliwości uszczegółowienia danych, które pozwalają dotrzeć do informacji przyspieszających identyfikację incydentu oraz umożliwiających analizę przyczyn, co przyczynia się do poprawy współpracy między personelem obsługi sieci i zespołem ds. bezpieczeństwa oraz szybszego rozwiązywania incydentów z zakresu zabezpieczeń.



Rys. 2. Sonar funkcjonujący w czasie rzeczywistym prezentuje ataki, które aktualnie mają miejsce w sieci. Ataki o wysokim stopniu ryzyka są zaznaczone bliżej nadajnika sonaru. Boczny wskaźnik podaje intensywność ruchu związanego z atakiem



Rys. 3. Przykład widoku najczęstszych ataków. Raport powstały w wyniku korelacji zdarzeń zebranych z wielu źródeł

Korzyści biznesowe

Utrzymanie ciągłości działań biznesowych nawet podczas ataku

- Pełna ochrona centrum danych i aplikacji do obsługi działalności biznesowej online przed znanymi i nowymi zagrożeniami sieciowymi
- Utrzymanie znakomitych czasów reakcji użytkowników nawet w przypadku zmasowanych ataków
- Zespół reagowania awaryjnego (ERT) wspierający klientów w przypadku szczególnie groźnych ataków

Zmniejszenie kosztów operacyjnych w zakresie zarządzania bezpieczeństwem

- Kontrola stanu zabezpieczeń w ujęciu biznesowym przy użyciu zintegrowanego mechanizmu SEM firmy Radware – przekładająca się na mniejszą złożoność i wyższe gwarancje bezpieczeństwa
- Zintegrowane rozwiązanie bezpieczeństwa – możliwość uniknięcia „martwych punktów” i duże oszczędności bez konieczności integracji narzędzi

Zmniejszenie wydatków kapitałowych na zabezpieczenia

- Wiele narzędzi bezpieczeństwa w jednym zintegrowanym rozwiązaniu

Radware AMS is based on the following Radware products:

DefensePro
Urządzenie zapobiegające atakom na sieć i serwery

AppWall
Zapora typu Web Application Firewall (WAF)

APSolute Vision
Mechanizm zarządzania oraz raportowania
i zapewnienia zgodności z zakresu bezpieczeństwa

Informacje o firmie Radware

Firma Radware (NASDAQ: RDWR) to globalny lider w zakresie tworzenia aplikacji i rozwiązań bezpieczeństwa aplikacyjnego dla centrów danych w modelach wirtualnych i w chmurze. Wielokrotnie nagradzana oferta produktów tej firmy gwarantuje pełną odporność dla zastosowań o kluczowym znaczeniu, maksymalną wydajność informatyczną oraz pełną elastyczność biznesową. Rozwiązania firmy Radware pracują już u ponad 10 000 klientów i operatorów na całym świecie, umożliwiając im szybkie adaptowanie się do wyzwań rynkowych, utrzymywanie ciągłości biznesowej oraz osiągnięcie maksymalnej produktywności przy jak najniższych kosztach. Więcej informacji można znaleźć pod adresem www.radware.com.

Program Certainty Support

Firma Radware oferuje wsparcie techniczne dla wszystkich swoich produktów w postaci programu Certainty Support. Każdy poziom programu Certainty Support składa się z czterech elementów – pomocy telefonicznej, aktualizacji oprogramowania, konserwacji sprzętu oraz interwencji na miejscu instalacji. Firma Radware dysponuje również specjalistycznym personelem technicznym, który może świadczyć klientom fachowe usługi w ramach zaawansowanych projektów wdrożeniowych.