Systemy monitorowania, kontroli dostępu i zarządzania sieciami

Sprawnie i wydajnie działająca sieć komputerowa jest obecnie niezbędnym elementem infrastruktury każdej firmy. Systemy bezpieczeństwa, takie jak firewall wraz z modułami wykrywania włamań (IDS/IDP) nie pokrywają całości potrzeb w zakresie utrzymania i zabezpieczenia sieci lokalnej, a tym bardziej sieci wielooddziałowych. Dodatkowym wyzwaniem są nowe technologie wdrażane w zakresie infrastruktury: chmura publiczna i prywatna, wirtualizacja serwerów oraz Software Defined Networking (SDN). Z drugiej strony nowe ustawodawstwo narzuca coraz bardziej restrykcyjne wymagania dotyczące ochrony danych, np. w zakresie danych osobowych: GDPR/RODO.

Współczesne sieci wymagają dodatkowych rozwiązań będących uzupełnieniem podstawowych funkcji bezpieczeństwa oferowanych przez systemy firewall - funkcjonalności takie oferują m.in. systemy monitorowania przepływów, systemy zdalnego dostępu oraz systemy monitorowania sesji i zarządzające dostępem.

Systemy monitorowania przepływów sieciowych

Systemy monitorowania przepływów pozwalają na dokładne poznanie w czasie rzeczywistym charakterystyki ruchu w sieci komputerowej, jakiej z racji swojego scentralizowanego charakteru nie zapewni system firewall. Poprzez zbieranie ruchu z wybranych segmentów sieci system monitorowania jest w stanie wykryć oraz zareagować na różnego rodzaju zagrożenia, takie jak: ataki DDoS, infekcje mallware, a także: awarie sprzętu, niepoprawne zachowanie aplikacji czy świadomie złośliwe działanie użytkowników. System monitorowania może też być bardzo przydatnym narzędziem służącym do optymalizacji wydajności łącz WAN oraz sieci LAN.

Systemy monitorowania zaopatrzone w moduł analizatora zachowania (NBA-Network Behavior Analysis) pozwalają na wyizolowanie konkretnych dozwolonych, zakazanych lub podejrzanych wzorców komunikacji i na odpowiednią reakcję, np. zablokowanie ruchu. Dodatkowo, system monitoringu może gromadzić historyczne dane dotyczące przepływów, co pozwala na przeprowadzenie efektywnej analizy powłamaniowej, np. w celu ustalenia źródła ataku oraz oszacowania stopnia zagrożeń dla danych.

Systemy zdalnego dostępu

Systemy zdalnego dostępu pozwalają na zrealizowanie bezpiecznego dostępu do wybranych serwisów, zasobów i aplikacji dla użytkowników zewnętrznych. Współczesne systemy zdalnego dostępu nie wymagają instalacji dedykowanego klienta VPN (lub też instalacja ta jest niezwykle uproszczona). Zakres dostępu może obejmować takie serwisy jak: wewnętrzne aplikacje WWW, pocztę elektroniczną, serwery plików, aplikacje Windows, a nawet dostęp do pulpitu wybranych komputerów. Jednocześnie realizowana jest kontrola dostępu i weryfikacja uprawnień w systemach wymagających podwyższonego poziomu bezpieczeństwa. Weryfikacja dostępu może obejmować takie mechanizmy jak weryfikacja tożsamości przy pomocy karty chipowej lub tokena sprzętowego.

Systemy monitorowania sesji

System monitorowania sesji pozwala na pełną kontrolę sesji realizowanych zarówno wewnątrz sieci LAN, jak i zdalnych (inicjowanych z Internetu). Systemy te pozwalają na kontrolę protokołów zdalnego dostępu takich jak: SSH, RDP, telnet, X11, HTTP/HTTPS. System monitorowania realizuje nadzór oraz nagrywanie sesji. Może też jednocześnie pełnić rolę pośrednika przy autoryzacji użytkowników, dzięki czemu zewnętrzni dostawcy nie muszą posiadać bezpośrednich poświadczeń bezpieczeństwa do naszych systemów. Monitorowanie sesji jest przydatnym narzędziem wszędzie tam, gdzie wiele osób i podmiotów (np. zewnętrzni dostawcy) posiada dostęp do różnorodnych systemów IT, a także we wszystkich zastosowaniach, w których kluczowa jest kontrola działania użytkowników uprzywilejowanych (administratorów, operatorów, itp.).

Niezawodność

Oferowane przez nas rozwiązania posiadają dożywotnią gwarancję i wsparcie producenta z opcją wymiany w trybie "next-day". Możliwe jest uruchomienie konfiguracji redundantnych, w których awaria jednego z komponentów nie powoduje przestoju w pracy systemu.
Oferujemy też pełen zakres usług serwisowych.

CC oferuje

W dziedzinie opisywanych rozwiązań dla monitoringu i dostępu sieciowego oferujemy nie tylko dostawy sprzętu, ale także pełną gamę usług: prowadzimy analizę potrzeb klientów, projektujemy sieci i serwerownie, realizujemy testy oraz diagnostykę istniejącej infrastruktury, wykonujemy częściowe lub pełne migracje rozwiązań sieciowych, wdrażamy i konfigurujemy nowy sprzęt, prowadzimy nadzór oraz utrzymanie w trybie 24x7, a także realizujemy szkolenia warsztatowe. Wszystkie usługi wykonywane są przez naszych pracowników posiadających certyfikaty inżynierów danego producenta - posiadamy i utrzymujemy aktualne certyfikacje wszystkich kluczowych, wymienionych niżej dostawców rozwiązań sieciowych.

Po co monitorować?

55% naruszeń bezpieczeństwa jest związanych z wykorzystaniem kont uprzywilejowanych, a 60% incydentów wynikało z błędów popełnionych przez administratorów (Źródło: Verizon "2015 Data Breach Investigation report"). Brak kontroli nad użytkownikami uprzywilejowanymi stwarza zagrożenie dla integralności i bezpieczeństwa danych.
Dodatkowo przejęcie dostępu do kont uprzywilejowanych przez osobę z zewnątrz może doprowadzić do wycieku danych lub kompromitacji przedsiębiorstwa.

Producenci:
Flowmon, Wheel, PulseSecure

Flowmon Driving Network Visibility
WHEEL SYSTEMS
Pulse Secure

CC
Otwarte Systemy
Komputerowe Sp. z o.o.

ul. Rakowiecka 36, 02-532 Warszawa
tel. +48 22 646-68-73; fax +48 22 606-37-80
e-mail: sales@cc.com.pl

Więcej informacji znajdziecie Państwo w Internecie, na stronach:
http://www.cc.com.pl/

Kontakt:
Kontakt ogólny: cc@cc.com.pl
Dział Handlowy: sales@cc.com.pl
Dział Techniczny: tech@cc.com.pl