

NETASQ

OKIEM MENEDŻERA



Współczesne wyzwania menedżera wobec technologii IT:

1. Obecnie najczęściej atak na infrastrukturę informatyczną firmy bezpośrednio uderza w jej reputację na rynku co ma bezpośrednie przełożenie na zaufanie jak i wyniki finansowe.
2. Internet choć niezbędny w pracy, na co dzień obniża jednak efektywność pracowników – wg badań pracownik spędza średnio nawet do 2 godzin na nieproduktywnych stronach WWW w czasie pracy. Ogromny wpływ na zmniejszenie produktywności mają również wiadomości spamowe.
3. Dział informatyki, chcąc dobrze zabezpieczyć infrastrukturę, niejednokrotnie proponuje wiele rozwiązań specjalistycznych, które są trudne do zaakceptowania z powodu wysokich kosztów zakupu, utrzymania jak i administracji, która dodatkowo wiąże się z poświęceniem dodatkowych pieniędzy i czasu na szkolenia z zakresu efektywnego wykorzystania tych rozwiązań.

Jak wdrożenie urządzenia UTM wpłynie na bezpieczeństwo i efektywność biznesową mojej firmy?

WZMOCNIENIE BEZPIECZEŃSTWA FIRMY I JEJ DANYCH:

1. NETASQ posiada autorski system ochrony przed włamaniami do sieci firmowej (ASQ), który jest w stanie powstrzymać nawet ataki przygotowywane pod kątem konkretnej firmy (w odróżnieniu od systemów IPS bazujących na sygnaturach, które w takich sytuacjach są bezradne).
2. Firewall zamyka próby nieuprawnionego dostępu z zewnątrz.
3. Jeśli firma posiada własny sklep internetowy lub serwis WWW – system ochrony przed włamaniami eliminuje również ataki na serwis internetowy firmy, co ma fundamentalne znaczenie dla wizerunku firmy (ochrona marki).
4. Z całego ruchu w sieci usuwane są wirusy – jest to dodatkowa warstwa ochrony poza programami antywirusowymi na poszczególnych komputerach.
5. Poprzez szczegółowy monitoring pracy każdego z pracowników zyskujemy szczegółowe informacje w przypadku prób sabotażu, prób nieuprawnionego dostępu wewnątrz firmy przez jej pracowników.
6. Eliminowane są z komputerów stare, nieaktualne wersje programów zawierających luki bezpieczeństwa – urządzenie zbiera informacje o takich przypadkach i raportuje takie zdarzenia administratorowi.

UNIKNIĘCIE PRAWNEJ ODPOWIEDZIALNOŚCI FIRMY:

1. Poprzez uszczelnienie dostępu do danych osobowych, bazy klientów – radykalnie zwiększa bezpieczeństwo danych.
2. Firma ponosi odpowiedzialność za instalację nielegalnego oprogramowania. NETASQ potrafi sprawdzać jakie programy łączą się z Internetem z poszczególnych komputerów – dzięki temu szybko można wykryć fakt samowolnego zainstalowania programu przez pracownika (o ile tylko łączy się z siecią).
3. W przypadku podjęcia nielegalnych działań przez pracownika firmy, zyskujemy szczegółowe raporty imienne o aktywności danej osoby w sieci (a nie tylko komputera – pod warunkiem integracji NETASQ z bazą użytkowników).

PODNIESIENIE EFEKTYWNOŚCI PRACY:

1. Urządzenie umożliwia zdalny dostęp pracowników do zasobów sieci firmowej – plików, poczty, systemu CRM itp. poprzez bezpieczne - szyfrowane tunele VPN (jako jedyny UTM posiada w tym zakresie certyfikat bezpieczeństwa UE na poziomie EU Restricted).
2. Urządzenie pozwala wybranym pracownikom i grupom blokować dostęp do stron niezwiązanych z pracą, zmniejszając ilość czasu „marnowanego” na bezproduktywną aktywność w Internecie (np. Allegro, Facebook, demotywatory, kwejk itd.) - NETASQ robi to lepiej niż większość urządzeń amerykańskiej konkurencji, ponieważ filtr stron internetowych został stworzony z udziałem polskiego dystrybutora na podstawie badań aktywności w Internecie pracowników polskich firm (konkurencja bazuje najczęściej na amerykańskich bazach stron WWW).
3. Pozwala odciąć pracownikom możliwość pobierania filmów przez sieci P2P, korzystania z komunikatorów (np. Skype).
4. Cały czas możemy w wybranych dniach, godzinach lub dla wybranych pracowników pozwalać na więcej – robić wyjątki w razie potrzeby.
5. W przypadku szczytu aktywności firmy (np. okres przedświąteczny) i dużego ruchu w sieci urządzenie umożliwia zachowanie płynności pracy najważniejszych działów – poprzez nadanie priorytetów ruchu w sieci np. e-mailom z zamówieniami, osobom obsługującym system CRM, a zmniejszenie wykorzystania łączy do mniej ważnych zadań (np. strony WWW).
6. Wylimitowanie niepożądanych e-maili (spamu).

KONTROLA PRACOWNIKÓW:

1. Menedżerowie mogą otrzymywać regularnie raporty o tym jakie strony, w jakich godzinach odwiedzał konkretny pracownik (nie tylko konkretny komputer), ile danych pobierał – wszystko w języku polskim i bez dodatkowych kosztów.
2. Raporty zawierają informacje, jakie aplikacje sieciowe pracownik zainstalował na swoim komputerze.
3. W razie potrzeby można niektóre grupy (np. zarząd) wyłączyć z monitorowania.
4. Istnieje możliwość wydzielenia odrębnej sieci dla gości bez dostępu do systemów wewnętrznych firmy (np. WiFi, gniazdka w pokojach do spotkań).

REDUKCJA KOSZTÓW:

1. Urządzenie NETASQ wykonuje funkcje różnych rozwiązań kupowanych zwykle dotąd osobno - jeśli zsumujemy łączny koszt dobrej klasy firewalla, systemu IPS, systemu filtrowania ruchu WWW, antyspamu i rozwiązań do kanałów VPN otrzymujemy koszt nawet kilkukrotnie wyższy niż wdrożenie rozwiązania klasy UTM.
2. Dzięki odcięciu możliwości korzystania z Internetu na cele niezwiązane z pracą, spada wykorzystanie łącza internetowego – mamy wtedy szybszy Internet do pracy i nie musimy kupować szybszych łączy (istnieją udokumentowane przypadki w dużych urzędach, gdzie ruch spadał nawet o 50%!).
3. W przypadku firmy z kilkoma oddziałami, wykorzystanie szyfrowanego tunelu VPN pomiędzy urządzeniami eliminuje konieczność dzierżawy drogich łączy od dostawców Internetu – taka inwestycja zwraca się w kilka miesięcy.