NETASQ | STORMSHIELD

STORMSHIELD
OKIEM MENEDŻERA

Współczesne wyzwania menedżera wobec technologii IT:

1. Obecnie atak na infrastrukturę informatyczną firmy najczęściej 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 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 oraz administracji. Zastosowanie wielu dedykowanych produktów to również konieczność poświęcenia dodatkowych pieniędzy i czasu na szkolenia z zakresu efektywnego wykorzystania tych rozwiązań.
4. Coraz częstszym problemem dla wielu firm i instytucji samorządowych oraz rządowych w Polsce jest szpiegostwo przemysłowe, polityczne i gospodarcze. Dzisiejsze ataki hakerskie kierowane są na konkretną sieć. Mają one za zadanie przede wszystkim wykraść dane osobowe i wrażliwe dane firmowe, takie jak bazy klientów jak również przekierować środki pieniężne na inne konta, wyłudzić pieniądze przy użyciu służbowych komputerów czy dokonać zmian na stronie internetowej. Udowodniono nie raz, że wielu amerykańskich czy chińskich producentów implementuje oprogramowanie szpiegujące w eksportowanym sprzęcie. Warto przy wyborze UTMa zwrócić uwagę czy dane rozwiązanie posiada europejskie certyfikaty bezpieczeństwa takie EU Restricted, NATO czy Common Criteria EAL 4+.

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

WZMOCNIENIE BEZPIECZEŃSTWA FIRMY I JEJ DANYCH:

1. STORMSHIELD 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 blokuje 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 i wrażliwych danych firmowych).
4. Urządzenie usuwa wirusy z ruchu przechodzącego w sieci firmowej – 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, a także prób nieuprawnionego dostępu wewnątrz firmy przez jej pracowników.
6. Urządzenie wykrywa na komputerach stare, nieaktualne wersje programów zawierające luki bezpieczeństwa – urządzenie zbiera informacje o takich przypadkach i raportuje takie zdarzenia administratorowi, który następnie może je usunąć.

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. STORMSHIELD 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 STORMSHIELD 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.) - STORMSHIELD robi to lepiej niż większość urządzeń konkurencji, ponieważ filtr stron internetowych został stworzony z udziałem polskiego dystrybutora, na podstawie badań aktywności w Internecie pracowników polskich firm (konkurencja bazuje najczęściej na zagranicznych bazach stron WWW).
3. Pozwala odciąć pracownikom możliwość pobierania danych przez sieci P2P (np. pirackich wersji oprogramowania, filmów oraz muzyki) oraz 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 łącz do mniej ważnych zadań (np. strony WWW).
6. Wyeliminowanie 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. Na tej podstawie można podjąć decyzję, jakie strony należy konkretnemu pracownikowi zablokować, aby poprawić jego efektywność pracy.
2. Raporty zawierają informacje, które aplikacje sieciowe zainstalowane na komputerze pracownika są podatne na zagrożenia.
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. Wi-Fi, gniazdka w pokojach do spotkań).

REDUKCJA KOSZTÓW:

1. Urządzenie STORMSHIELD wykonuje funkcje różnych rozwiązań kupowanych zwykle 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 rozwiązań STORMSHIELD.
2. Dzięki odcięciu możliwości korzystania z Internetu w celach niezwiązanych z pracą, spada wykorzystanie łącza internetowego – mamy wtedy szybszy Internet do pracy i nie musimy kupować szybszych łącz (istnieją 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 łącz od dostawców Internetu – taka inwestycja zwraca się w kilka miesięcy.

Dystrybucja w Polsce:
DAGMA Biuro Bezpieczeństwa IT | ul. Bażantów 4/2 | 40-668 Katowice
tel. 32 793 11 00 | faks 32 793 11 90 | www.stormshield.pl | kontakt@stormshield.pl