Czy jesteś spokojny o swoje dane, przeglądając strony internetowe? Możesz myśleć, że jesteś bezpieczny, ale z odkrywanymi co kilka sekund nowymi zainfekowanymi witrynami, bycie na bieżąco jest praktycznie niemożliwe - niezależnie od tego, jaką wiedzę posiadasz lub jak bardzo jesteś świadom zagrożeń.

Czy praktykujesz bezpieczne przeglądanie sieci? Unikasz niebezpiecznych witryn? Ograniczasz czas online pracy? Stosujesz solidną politykę dostępu do Internetu? Korzystasz z bezpiecznej przeglądarki? Potrafisz zidentyfikować niebezpieczną witrynę, gdy się na taką natkniesz? Jeśli odpowiedziałeś twierdząco na którekolwiek z powyższych pytań, powinieneś przeczytać ciąg dalszy raportu.

Prawdopodobnie masz błędne wyobrażenie na temat bezpieczeństwa w sieci, ale nie martw się - nie jesteś sam. W ciągu ostatnich kilku lat, wiele niewłaściwych informacji krążyło zarówno na temat zagrożeń jak i sposobów jak się przed nimi chronić. Sophos, firma specjalizująca się w technologiach ochrony informacji, przedstawia listę mitów bezpiecznego surfowania:

Mit nr 1: Internet jest bezpieczny, ponieważ mój komputer nigdy nie został zainfekowany złośliwym oprogramowaniem

Możesz nawet nie zdawać sobie sprawy z tego, że na twoim pececie znajduje się niebezpieczny kod. Wiele sieciowych ataków malware jest zaprojektowanych tak, by ukraść dane osobiste, hasła lub wykorzystać twoją maszynę do rozsyłania spamu.

Mit nr 2: Użytkownicy nie marnują czasu na nieodpowiednich stronach internetowych

Bez żadnego narzędzia do filtrowania sieci, nie masz pojęcia, jak użytkownicy wykorzystują dostęp do Internetu. Faktem jest, że ponad 40% połączeń sieciowych w pracy odbywa się w niewłaściwym celu - średnio od 1 do 2 godzin dziennie na użytkownika.

Mit nr 3: Kontroluję korzystanie z Internetu i użytkownicy nie mogą obejść mojej polityki bezpieczeństwa

Korzystanie z anonimowego proxy ułatwia pracownikom omijanie filtrowania sieci i pozwala odwiedzić jakąkolwiek witrynę. Anonimowe proxy są łatwo dostępne i często używane, nawet przez dzieci w szkołach.

Mit nr 4: Tylko strony o tematyce pornograficznej i hazardowej są niebezpieczne

Zhakowane zaufane witryny stanowią ponad 83% stron udostępniających malware. Większość zainfekowanych stron to te, które odwiedzamy codziennie i ufamy ich zawartości.

Mit nr 5: Tylko naiwni użytkownicy dają się zainfekować złośliwym oprogramowaniem i wirusami

Malware z zainfekowanych stron pobiera się automatycznie, bez interwencji użytkownika, wystarczy odwiedzić niebezpieczną witrynę. Dlatego nie ma znaczenia, jaką wiedzę na temat komputerów posiadasz - gdy natkniesz się na taką stronę, jesteś w niebezpieczeństwie.

Mir nr 6: Możesz zainfekować komputer tylko poprzez pobieranie plików

Większość infekcji złośliwym oprogramowaniem następuje w wyniku wejścia na stronę, w której kodzie hakerzy umieścili niebezpieczny kod.

Mit nr 7: Firefox jest bezpieczniejszy od Internet Explorera

Wszystkie przeglądarki są w równym stopniu narażone na niebezpieczeństwa, ponieważ wszystkie zasadniczo są środowiskiem dla uruchamiania kodu JavaScript - języka programowania stosowanego głównie na stronach internetowych, wykorzystywanego również przez autorów złośliwego kodu. Ponadto, wiele exploitów bazuje na wtyczkach dostępnych dla każdej przeglądarki, np. Adobe Acrobat Reader. Jedno jest pewne, nie ma całkowicie bezpiecznej przeglądarki.

Mit nr 8: Gdy w przeglądarce pojawia się ikona kłódki, jest bezpiecznie

Ikona kłódki wskazuje, że połączenie między przeglądarką a serwerem jest szyfrowane, co pomaga chronić nasze poufne dane osobiste przed przechwyceniem. To nie wyklucza jednak zagrożeń płynących z malware. Większość produktów internet security jest całkowicie ślepa jeśli chodzi o szyfrowane połączenia: to idealna szansa dla złośliwego oprogramowania do infiltracji naszej maszyny. Ponadto, niektóre szkodliwe programy mogą wykorzystać luki w zabezpieczeniach do podrobienia certyfikatów SSL. Hakerzy umieszczają je na fałszywych stronach bankowych w celu wyłudzenia pieniędzy - dla przeciętnego użytkownika, tak spreparowane witryny są trudne do zweryfikowania.

Mit nr 9: Bezpieczeństwo w sieci wymaga kompromisu między bezpieczeństwem, a wolnością

Podczas gdy Internet stał się krytycznym narzędziem dla wielu pracowników, Facebook dla działów HR czy Twitter dla PR-u, jakikolwiek kompromis między dostępem, a bezpieczeństwem nie wchodzi w grę. Odpowiednie rozwiązanie typu web security zapewnia możliwość swobodnego surfowanie przy jednoczesnym zachowaniu bezpieczeństwa.

Mit nr 10: Rozwiązania bezpieczeństwa na punktach końcowych nie chronią przed zagrożeniami z sieci

Zazwyczaj tak jest, ponieważ przeglądarka jest swoim środowiskiem uruchomieniowym: pobiera zawartość, przetwarza ją i wykonuje skrypty, wszystko bez widoczności na zewnątrz, szczególnie dla produktów typu endpoint security. Jednak to się zmienia. Narzędzie Sophos Live Protection Web Filtering, które jest częścią pakietu Endpoint Security and Control 9.5 pozwala w czasie rzeczywistym na filtrowanie złośliwych witryn na punktach końcowych.

Kompletny raport jest dostępny do pobrania za darmo na stronie Sophos pod adresem:
http://www.sophos.com/security/topic/web-security-myths.html

Sophos