

Sophos przedstawia raport największych zagrożeń 2009

Autor: Serchio
03.02.2010.

SOPHOS

Sophos, firma specjalizująca się w technologiach ochrony informacji, opublikował raport ujawniający niepokojący wzrost liczby ataków cyberprzestępców na użytkowników sieci społecznościowych, takich jak Facebook czy Twitter.

Badanie firmy Sophos pokazuje, że w ciągu minionych 12 miesięcy przestępcy skoncentrowali swoje ataki na użytkownikach portali społecznościowych:

* 57% użytkowników doniosło o atakach spamu przez portale społecznościowe, wzrost o 70,6% w stosunku do poprzedniego roku

* 36% otrzymało oprogramowanie typu malware za pośrednictwem sieci społecznościowych, to wzrost o 69,8% w porównaniu do minionego roku

"Internauci spędzają na portalach społecznościowych coraz więcej czasu, dzieląc się cennymi informacjami osobistymi, a hakerzy tylko czekają na okazję do ataku," powiedział Graham Cluley, starszy konsultant ds. technologii w Sophos. "Dramatyczny wzrost ilości ataków w minionym roku mówi nam, że sieci społecznościowe oraz miliony ich użytkowników muszą robić więcej, aby chronić się przed cyberprzestępczością, próbami kradzieży tożsamości, scamem oraz atakami malware."

72% firm jest zdania, że ich pracownicy narażają na portalach społecznościowych swoje firmy na szwank

W badaniu Sophos wzięło udział ponad 500 organizacji. Okazało się, że aż 72% firm zaniepokojona jest zachowaniem swoich pracowników na portalach społecznościowych, które naraża ich biznes oraz cenne dane.

Badanie bezpieczeństwa sieci społecznościowych to zaledwie jedna część raportu zagrożeń Sophos 2010, który zgłębia obecne trendy w bezpieczeństwie. Raport ujawnia, że przestępcy identyfikują potencjalne ofiary na sieciach społecznościowych, a następnie atakują ze zdwojoną siłą - w domu i w pracy. Zdaniem specjalistów z Sophos, wiele stron Web 2.0 za bardzo koncentruje się na zagarnięciu jak największej części rynku, zamiast chronić swoich użytkowników przed internetowymi zagrożeniami.

Facebook - najstraszniejsza sieć społecznościowa?

Respondenci byli także zapytani o to, którą sieć społecznościową uważają za najniebezpieczniejszą. Aż 60% podało, że jest nią Facebook:

- * 1. Facebook: 60%
- * 2. MySpace: 18%
- * 3. Twitter: 17%
- * 4. LinkedIn: 4%

"Nie powinniśmy zapominać, że Facebook jest, jak dotąd, największą siecią społecznościową - i w największym sadzie znajdzie się więcej zepsutych jabłek," wyjaśnił Cluley. "Prawda jest taka, że grupa odpowiedzialna za bezpieczeństwo Facebooka daje z siebie wszystko, aby stawić czoła zagrożeniom na ich stronie - chodzi o to, że kontrola nad 350 milionami użytkowników nie jest łatwym zadaniem dla nikogo. Ale nie ma wątpliwości, że proste zmiany mogłyby podnieść bezpieczeństwo użytkowników Facebooka. Na przykład, gdy Facebook wprowadził w grudniu 2009 nowe zalecane ustawienia prywatności, był to krok wstecz, zachęcający wielu użytkowników do udostępniania swoich informacji każdemu w sieci."

Raport zagrożeń Sophos pokazuje również, że 49% firm pozwala swoim pracownikom na swobodny dostęp do Facebooka, to 13% wzrost w stosunku do poprzedniego roku.

"Ironia polega na tym, że wraz z rozluźnieniem nastawienia firm do aktywności pracowników na sieciach społecznościowych, rośnie ilość ataków phishingowych, spamu, malware i kradzieży tożsamości na Facebooku," powiedział Cluley. "Jednak sieci społecznościowe mogą odgrywać bardzo ważną rolę w dzisiejszym biznesie i sęk w tym, żeby nauczyć pracowników zasad bezpieczeństwa zamiast odcinać im dostęp do portali."

LinkedIn - dostarczyć hakerom firmowe dane

Mimo, że LinkedIn uważany jest za najmniej groźną sieć, Sophos radzi, aby zachować ostrożność, ponieważ za pośrednictwem portalu można przekazać pokaźną pulę danych hakerom.

"Ataki wycelowane w przedsiębiorstwa to w chwili obecnej duży problem, im więcej informacji przestępca zdobędzie o strukturze organizacji, tym łatwiej będzie mu wysłać zainfekowany załącznik do konkretnej osoby i komputera," wyjaśnił Cluley. "Strony jak LinkedIn dostarczają hakerom swego rodzaju katalog firmowy, zawierający nazwiska i stanowiska pracowników. To sprawia, że dotarcie do adresów email ofiar, jest dziecinnie proste."