Co robić kiedy padłeś ofiarą przestępcy internetowego?

Kategoria: Styl życia
Opublikowano: sobota, 29, grudzień 2012 23:00
Rafał Rudka

Bez względu na to ile kroków podjąłeś aby ochronić siebie i swoje informacje, wciąż istnieje szansa, że staniesz się ofiarą przestępstwa internetowego. Podobnie jak z prowadzeniem samochodu - nie ważne jak jesteś ostrożny, prędzej czy później, najprawdopodobniej będziesz miał stłuczkę. Jednak, pomimo tego, nawet po dokonanym włamaniu, nadal można się zabezpieczyć. Im wcześniej takie zdarzenie zostanie wykryte i im szybsza będzie reakcja, tym większa jest szansa na zmniejszenie szkód.

Aby pomóc Ci się przygotować, omówimy różne sposoby sprawdzenia czy komputery, konta bankowe lub inne informacje zostały naruszone oraz jak można najlepiej w danej sytuacji zareagować. Większość naszych porad dotyczy kroków, które należy podjąć w przypadku zaatakowania komputera osobistego. Jeśli zaatakowane zostało urządzenie służbowe, lub takie gdzie było konto służbowe lub istnieje obawa, że ktoś mógł uzyskać dostęp do firmowych informacji, należy natychmiast zgłosić incydent do zespołu pomocy w swojej organizacji lub zespołu bezpieczeństwa, a następnie postępować zgodnie z ich instrukcjami.

Twoje konta

Prawdopodobnie posiadasz wiele różnych kont internetowych, poprzez które uzyskujesz dostęp do wielu usług od bankowości elektronicznej, poprzez sklepy internetowe, pocztę i portale społecznościowe. Śledzenie każdego z nich a do tego zauważenie, kiedy konto jest narażone na niebezpieczeństwo, może być nie lada wyzwaniem. Oto kilka kroków, które pomogą Ci zidentyfikować i zareagować w przypadku skompromitowania któregoś z kont.

Objawy:

- Nie można zalogować się na stronie internetowej, nawet jeśli jesteś pewien, że wpisywane hasło jest prawidłowe.
- Twoi przyjaciele lub współpracownicy otrzymują od Ciebie e-maile, które nigdy nie zostały przez Ciebie wysłane.
- Ktoś zamieszcza w Twoim imieniu wiadomości na stronach sieci społecznościowych (takich jak Facebook czy Twitter).
- Ktoś przelewa pieniądze z Twojego internetowego konta bankowego.
- Dane kontaktowe lub inne ustawienia na kontach internetowych są zmieniane bez Twojej wiedzy i zgody.
- Strona internetowa lub dostawca usług podaje do publicznej wiadomości, że dokonano włamania a więc konta i hasła użytkowników zostały narażone na niebezpieczeństwo.

Reakcja:

- Jeśli jednak wciąż możesz się zalogować, natychmiast zmień hasło. Jak zawsze pamiętaj, że należy używać silnych haseł.
- Jeśli nie możesz się zalogować, natychmiast skontaktuj się z usługodawcą lub stroną internetową. Większość dostawców usług internetowych zapewnia jakiś sposób aby można było ich powiadomić, że Twoje konto zostało skompromitowane. Może to być formularz kontaktowy, adres e-mail lub numer telefonu.
- Po odzyskaniu dostępu, przejrzyj wszystkie ustawienia konta, aby upewnić się, że nic nie zostało zmienione przez włamywacza.
- Upewnij się, że zmieniłeś hasło na wszystkich innych kontach, do których było używane to samo

co w skompromitowanym serwisie.

Twoje urządzenia

Wraz z eksplozją popularności urządzeń mobilnych, teraz mamy jeszcze więcej rzeczy do ochrony. Kiedy napastnicy przejmą kontrolę nad urządzeniem, mają zdolność do przechwytywania każdego działania jakie można na nim wykonać. Oto kilka kroków, które pomogą Ci zidentyfikować i zareagować w przypadku zainfekowania urządzenia.

Objawy

- Komputer zabiera Cię na strony internetowe na które nie chcesz się udać.
- Komputer uruchamia programy, które nigdy nie były zainstalowane.
- Oprogramowanie antywirusowe zgłasza zainfekowany plik.
- Aktualizacje antywirusa i systemu kończą się niepowodzeniem.
- Urządzenie wciąż się zawiesza.
- Twój telefon wykonuje kosztowne połączenie lub zakupuje aplikacje bez Twojej zgody.

Im wcześniej zorientujesz się, że padłeś ofiarą ataku, tym szybciej będziesz mógł zareagować i zminimalizować szkody.

Reakcja:

- Wykonaj pełne skanowanie zaktualizowanym programem antywirusowym. Jeśli wykryje jakiekolwiek zainfekowane pliki, wykonaj zalecane kroki. Możesz rozważyć uruchomienie dodatkowego skanowania zabezpieczeń przez skanery on-line.
- Jeśli urządzenie nie może zostać zabezpieczone przez oprogramowanie lub gdy chcesz się upewnić, że w pełni odzyskasz nad nim kontrolę, rozważ ponownie zainstalowanie systemu operacyjnego lub wykonanie pełnego resetu fabrycznego, zainstalowanie najnowszej wersji antywirusa oraz odzyskiwanie danych z kopii zapasowej (robisz regularnie kopie zapasowe danych osobowych, prawda?).

Twoje dane

Ochrona własnych informacji, takich jak numer PESEL, historii medycznej, czy historii zakupów jest trudne, ponieważ często trudno kontrolować te wszystkie dane. To organizacje takie jak dostawcy usług opieki zdrowotnej, wystawcy kart kredytowych, urzędy czy szkoły przechowują i operują tymi danymi. Oto kilka kroków, które pomogą Ci określić, kiedy dane osobowe zostały ujawnione i jak reagować.

Objawy

- Usługodawca oficjalnie informuje, że zdarzył się atak i Twoje dane (takie jak numer karty kredytowej) mogły zostać ujawnione.
- Zauważyłeś nieupoważnione obciążenia na karcie kredytowej.
- Raporty kredytowe wskazują złożenie wniosków kredytowych, których nie rozpoznajesz.
- Firma zapewniająca opiekę zdrowotną zwraca się o zapłatę za zabiegi, których nie przeszedłeś.
- Otrzymujesz listy ponaglające za zaległe płatności na rachunkach, które nigdy otworzyłeś.

Reakcja:

- Zadzwoń natychmiast do wystawcy karty kredytowej. Poproś o zastrzeżenie karty i wydanie nowej. Jest to usługa którą wystawca karty powinien oferować bezpłatnie.
- Skontaktuj się z operatorem usługi. Na przykład, jeśli podejrzewasz że oszustwo ma związek z rachunkiem ubezpieczeń lub kontem bankowym, należy zadzwonić do firmy ubezpieczeniowej lub banku.
- Podczas dokonywania każdego zgłoszenia, zawsze dokumentuj wszystkie rozmowy wraz z datą, godziną i nazwiskiem osoby, z którą rozmawiałeś. Zachowaj kopie całej korespondencji tekstowej.

Źródło: Biuletyn Bezpieczeństwa Komputerowego OUCH!, wrzesień 2012