SANS SECURITY AWARENESS

Biuletyn Bezpiecze stwa Komputerowego

Jestem ofiarą hakera?

Wstęp

Nie ma znaczenia jak bardzo starasz się być bezpieczny korzystając z komputera, czasami nasze bezpieczeństwo jest zagrożone i nic nie możemy na to poradzić. Analogicznie jak w przypadku jazdy samochodem, nieważne jak dobrze prowadzisz i tak możesz stać się ofiarą wypadku. Ponisze wskazówki pomogą Ci stwierdzić czy jesteś ofiarą hakera. Im szybciej wykryjesz włamanie i podejmiesz odpowiednie działania, tym mniej szkód wyrządzi atakujący.

Na co zwrócić uwagę?

Twój program antywirusowy zgłosił alert infekcji. Upewnij się czy powiadomienie naprawdę pochodzi z programu antywirusowego. Może się zdarzyć, że okno powiadomienia pochodzi z przeglądarki internetowej. Atakujący w ten sposób mogą wymusić na Tobie podjęcie działań np. wykonania połączenia telefonicznego na wyświetlany numer, bądź zainstalowania dodatkowego oprogramowania. Jeśli nie jesteś pewny skąd pochodzi powiadomienie, sprawdź to w swoim programie antywirusowym.

Otrzymałeś informację wskazującą na to, że Twoje dane na komputerze zostały zaszyfrowane i aby uzyskać ponowny dostęp do swoich plików musisz zapłacić odpowiednią kwotę.

Przeglądarka internetowa samoczynnie otwiera strony bez Twojej woli.

Programy na Twoim komputerze często się zawieszają oraz co chwilę wyskakują dziwne okna aplikacji.

Hasło logowania do systemu lub kont online przestało działać pomimo, że masz 100% pewność, że jest poprawne.

Znajomi zgłaszają Ci, że wysyłasz bardzo dużo spamu, chociaż wiesz, że nic takiego nie robiłeś.

Z Twojej karty kredytowej bądź konta bankowego dokonano transakcji, o której nie masz pojęcia.

Jak zareagować?

Jeśli podejrzewasz, że ktoś uzyskał nieautoryzowany dostęp do Twojego komputera, podejmij odpowiednie działania najszybciej jak tylko możesz. Jeśli incydent jest związany z miejscem Twojej pracy, nie staraj się naprawiać problemu na własną rękę. Poinformuj natychmiast o tym swojego pracodawcę. Jednakże jeśli włamanie miało miejsce na urządzeniu osobistym, bądź dotyczy prywatnych kont w serwisach społecznościowych, to poniżej znajduje się kilka informacji, które pomogą Ci walczyć z infekcjami.

Zmiana haseł: Pamiętaj, żeby zmienić wszystkie swoje hasła. Nie tylko hasła, których używasz do logowania na komputerze czy innych urządzeniach, ale także te do serwisów internetowych. Pamiętaj, aby robić to z innego komputera, o którym wiesz, że jest bezpieczny. Jeśli masz wiele kont zacznij od najważniejszych. Nie używaj jednego hasła do więcej niż jednego serwisu. Jeśli masz problem z zapamiętaniem wszystkich haseł, użyj menadżera haseł.

Finanse: W przypadku problemów z kartą kredytową bądź kontem bankowym, skontaktuj się natychmiast z bankiem lub firmą obsługującą Twoją kartę kredytową. Numer telefonu możesz znaleźć np. na tylnej części karty kredytowej, na wyciągu bankowy lub na stronie internetowej banku.

Program antywirusowy: Jeśli program antywirusowy powiadomił Cię o infekcji, najlepiej jest wykonać kroki, które doradza. Większość programów antywirusowych udostępnia link do strony, gdzie znajdziesz informacje na temat wykrytego zagrożenia.

Powtórna instalacja: Jeśli nie możesz naprawić zainfekowanego komputera lub chcesz mieć pewność, że jest on bezpieczny, najlepszym rozwiązaniem jest zainstalować system operacyjny od nowa. Nie powinieneś przywracać systemu z kopii zapasowej, gdyż ona również może być zainfekowana. Posłuż się kopią zapasową do odzyskania swoich prywatnych danych. Jeśli nie czujesz się na siłach przeinstalować system operacyjny, zastanów się czy nie poprosić o pomoc profesjonalisty. Jeśli Twój komputer jest już stary, to łatwiejszym rozwiązaniem może się okazać zakup nowego urządzenia. Niezależnie czy zainstalujesz system operacyjny powtórnie bądź zakupisz nowe urządzenie, upewnij się że oprogramowanie jest aktualne a funkcja automatycznej aktualizacji włączona.

Kopie zapasowe: Kluczowym krokiem, który pomoże Ci się przygotować na wypadek włamania jest właściwie robiona kopia bezpieczeństwa plików. Istnieje wiele rozwiązań, które automatycznie tworzą kopie zapasową codziennie lub nawet co godzinę. Niezależnie jakiego rozwiązania użyjesz, kopie muszą być robione regularnie. Powinieneś sprawdzać czy zostały wykonane poprawnie i czy da się przywrócić dane w nich zawarte. Dosyć często okazuje się, że po infekcji trzeba usunąć wszystkie dane z komputera i zainstalować system operacyjny na nowo. W takiej sytuacji kopie bezpieczeństwa pomogą Ci przywrócić Twoje osobiste dane.

Policja: Jeżeli uważasz, że padłeś ofiarą cyberprzestępców, zgłoś zawiadomienie o popełnieniu przestępstwa w jednostce Policji lub w prokuraturze, najlepiej najbliższej Twojego miejsca zamieszkania lub miejsca, w którym w danym momencie się znajdujesz.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK, powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.
WWW: http://www.cert.pl
Twitter: @CERT_Polska
Facebook: http://facebook.com/CERT.Polska

Redaktor Gościnny

Dr Johannes Ullrich *(@johullrich) jest dziekanem wydziału badań SANS Technology Institute. Sprawuje funkcję dyrektora SANS Internet Storm Center oraz posiada tytuł SANS Fellow. Stworzył system DShield, który monitoruje zdarzenia bezpieczeństwa w sieci. Odpowiedzialny jest za codzienne publikowanie wiadomości bezpieczeństwa komputerowego w serwisie Internet Storm Center.*

Przydatne linki

Kopie zapasowe:	https://www.sans.org/u/JGP
Bezpieczne hasła:	https://www.sans.org/u/JGU
Menadżer haseł:	https://www.sans.org/u/JGZ
Czym jest złośliwe oprogramowanie:	https://www.sans.org/u/JH4