OUCH! Luty 2021

Biuletyn Bezpieczeństwa Komputerowego

Zhakowali mnie. Co teraz?

Czy jestem ofiarą hakera?

Nie ma znaczenia jak bardzo starasz się być bezpieczny, korzystając z komputera, wcześniej czy później możesz zostać zaatakowany. Poniżej przedstawiamy kilka wskazówek, które świadczą o tym że mogłeś zostać zhakowany i co z tym zrobić.

Konta online

- Rodzina lub przyjaciele zwracają ci uwagę, że otrzymują od ciebie nietypowe wiadomości bądź zaproszenia, choć masz pewność, że ich nie wysyłałeś.
- Hasło do konta nie działa, nawet jeśli wiesz, że jest prawidłowe.
- Otrzymujesz powiadomienia o zalogowaniu na konto, chociaż wiesz, że tego nie robiłeś. Nigdy nie klikaj w łącza internetowe zawarte w takich powiadomieniach. Lepszą opcją będzie zalogowanie się na konto wpisując adres w przeglądarce internetowej, używając wcześniej zapisanej zakładki bądź przy pomocy aplikacji mobilnej.

Komputer i smartfon

- Program antywirusowy wysyła powiadomienia o zainfekowaniu systemu. Upewnij się, że powiadomienia generowane są przez program antywirusowy i nie są to przypadkowe wyskakujące okienka ze strony internetowej, nakłaniające do podjęcia działań takich jak zainstalowanie dodatkowego oprogramowania. Nie masz pewności? Uruchom program antywirusowy i sprawdź, czy komputer na pewno jest zainfekowany.
- Otrzymujesz powiadomienie, że pliki przechowywane na komputerze zostały zaszyfrowane i musisz zapłacić okup aby odzyskać do nich dostęp.
- Komputer wyraźnie spowolnił swoją pracę i wszelkie programy uruchomiają się dłużej niż zazwyczaj.
- Podczas przeglądania stron internetowych często następuje przekierowanie na inne strony, których nie chciałeś odwiedzić lub pojawiają się nowe, niechciane strony internetowe.

Finanse

- Zauważasz podejrzane, nieautoryzowane transakcje na karcie kredytowej lub koncie bankowym.

Co teraz? Jak odzyskać kontrolę

Jeśli podejrzewasz, że zostałeś zhakowany, zachowaj spokój. Jeśli problem wystąpił w miejscu pracy bądź na urządzeniu służbowym, nie próbuj naprawiać problemu na własną rękę. Zgłoś problem swojemu przełożonemu. Jeśli jest to urządzenie lub konto prywatne, wypróbuj kilka kroków, które możesz podjąć:

- **Odzyskanie konta online:** Jeśli nadal masz dostęp do konta, zaloguj się z zaufanego komputera, który na pewno nie jest zainfekowany i zresetuj hasło. Po zalogowaniu się, upewnij się, że ustawiłeś nowe, unikalne i silne hasło. Im dłuższe tym lepsze. Pamiętaj, że do każdego z kont powinno się używać innego hasła. Jeśli masz problem z zapamiętaniem wszystkich haseł, zalecamy skorzystanie z menedżera haseł. Włącz opcję uwierzytelnienia dwuskładnikowego, wszędzie gdzie to tylko możliwe. Jeśli nie masz dostępu do konta, skontaktuj się z serwisem i poinformuj go, że Twoje konto zostało przejęte lub skorzystaj z formularza pomocy zawierającego wskazówki co w takiej sytuacji poczynić.
- **Odzyskiwanie urządzeń:** W sytuacji kiedy program antywirusowy nie był w stanie naprawić zainfekowanego komputera lub jeśli chcesz mieć pewność, że urządzenie jest wolne od wirusów, rozważ reinstalacje systemu operacyjnego. Zazwyczaj wiąże się to z usunięciem wszystkich danych z dysku twardego urządzenia, a następnie ponownej instalacji i aktualizacji systemu operacyjnego. Nie należy instalować systemu operacyjnego z kopii zapasowych. Kopie zapasowe powinny być używane tylko do odzyskiwania plików osobistych. Jeśli nie czujesz się na siłach przeinstalowania systemu operacyjnego, rozważ skorzystanie z usług serwisu. Zastanów się również czy urządzenie, które posiadasz przypadkiem nie jest przestarzałe. Czasami taniej będzie kupić nowy sprzęt.
- **Odzyskiwanie kont bankowych:** W przypadku problemów z kartą kredytową lub kontem bankowym, należy niezwłocznie skontaktować się z bankiem lub firmą obsługującą kartę kredytową. Zadzwoń do nich używając zaufanego numeru telefonu, znajdującego się na odwrocie karty płatniczej, wydrukowanego na zestawieniu operacji lub widocznego na stronie internetowej. Monitoruj swoje transakcje regularnie, aby wczas zareagować na nieautoryzowane płatności. Rozważ również możliwość skorzystania z usługi Credit Freeze.

Jeśli czujesz się oszukany lub poniosłeś straty, zgłoś sprawę do organów ścigania.

Redaktor gościnny

Maxim Deweerdt (Twitter @alfasec) jest certyfikowanym instruktorem w Instytucie SANS, prowadzącym głównie kursy z Cyberobrony. Jest również głównym konsultantem w NVISO, gdzie koncentruje się na projektach dotyczących poszukiwań zagrożeń, reagowania na incydenty w sieci i sprawności zespołów SOC.

Źródła

Moc aktualizacji: : https://www.sans.org/security-awareness-training/resources/power-updating
Czy robisz kopie zapasowe? https://www.sans.org/security-awareness-training/resources/got-backups
Tworzenie haseł w prostszy sposób: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Ransomware: https://www.sans.org/security-awareness-training/resources/ransomware
Raport Identity Theft: https://www.identitytheft.gov
Credit Freezes: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz