OUCH! | Listopad 2013

Biuletyn Bezpieczeństwa Komputerowego

OUCH!

W TYM NUMERZE..

- **Sklepy online**
- **Bezpieczny komputer**
- **Karta kredytowa**

Bezpieczne zakupy w sieci

Gorący okres zakupowy

Zbliża się okres w roku, w którym przestajemy liczyć się z pieniędzmi i zaczynamy poszukiwania prezentów dla rodziny i przyjaciół. Wielu z nas, chcąc uniknąć kolejek albo poszukując okazji, wybiera zakupy online. Niestety jest to także czas, w którym cyber-złodzieje zaczynają intensywniej pracować poprzez przygotowywanie fałszywych sklepów i serwisów, wykradanie numerów kart kredytowych lub zwykłe oszustwa w postaci nie dostarczania zamówionych towarów. W tym numerze OCUH! opisujemy niektóre z zagrożeń związanych z zakupami online oraz przedstawiamy kilka metod, jak chronić się przed oszustami.

Redaktor gościnny

Redaktorem tego wydania magazynu OUCH! jest Lenny Zeltser, wykładowca Instytutu SANS prowadzący kurs analizy powłamaniowej ze szczególnym zwróceniem uwagi na użyte do ataku złośliwe oprogramowanie. Lenny pracuje także w firmie NCR Corp, gdzie zajmuje się bezpieczeństwem IT.

Sklepy online

Oszust internetowy może z łatwością stworzyć fałszywą stronę internetową, która będzie wyglądać identycznie jak dobrze nam znane serwisy aukcyjne albo sklepy w sieci. Gdy taka strona już funkcjonuje, oszuści starają się przyciągnąć do niej użytkowników wystawiając oferty, które są znacznie bardziej korzystne cenowo niż w prawdziwych sklepach. Szukając najlepszych cen na jakiś produkt, często używamy wyszukiwarek, takich jak Google albo Bing, dodając do nazwy poszukiwanej rzeczy słowa takie jak “okazja”, “najlepsza cena” lub “najtaniej”. Wyszukiwarki potrafią zwrócić tysiące wyników, zwłaszcza jeśli szukany produkt jest czymś popularnym. Musimy pamiętać, że część z nich może prowadzić do fałszywych stron, które próbują nas okraść.

Wybierając sklep internetowy albo serwis aukcyjny w celu kupna jakiejś rzeczy, bądźmy szczególnie ostrożni w przypadku tych, które oferują niesamowite promocje w porównaniu do innych, dobrze znanych marek. Powodem, dla którego różnica w cenie może być aż tak wielka jest to, że po zakupie możemy otrzymać nie oryginalną rzecz a podróbkę, coś co było wcześniej skradzione, albo po prostu nie otrzymać nic. Szukając okazji zwróć szczególną uwagę na pewne cechy serwisu internetowego, które mogą sugerować, aby trzymać się od niego z daleka:

- Na stronie nie jest podany numer telefonu, aby skontaktować się z działem sprzedaży lub innym do którego można skierować pytania.
- Adres strony internetowej znacząco różni się od tego wykorzystywanego do komunikacji za pomocą poczty elektronicznej.
- Na stronie internetowej możesz odnaleźć wiele rażących błędów gramatycznych lub językowych.
- Strona internetowa z okazją do złudzenia przypomina stronę innego dobrze znanego i

Bezpieczne zakupy w sieci

sprawdzonego sklepu internetowego lub serwisu aukcyjnego, ale jej adres różni się od oryginalnego tylko w niewielkim stopniu (np. jedną literą).

Pamiętaj o jednej kwestii - to, że strona internetowa jest profesjonalnie przygotowana i graficznie wygląda świetnie, nie oznacza od razu, że jest prawdziwa i należy jej bezgranicznie wierzyć. Jeśli jakiś aspekt serwisu wydaje Ci się podejrzany, lepiej poświęcić trochę więcej czasu na sprawdzenie, czy sklep nie jest próbą oszustwa i mieć pewność, że nie stracimy naszych pieniędzy. Dla przykładu, możesz spróbować zadzwonić na numer telefonu, który powinien być umieszczony w sekcji kontakt i sprawdzić, czy jest prawdziwy. Dodatkowo powinieneś wpisać w wyszukiwarkę nazwę sklepu albo jej adres internetowy i sprawdzić jakie ma opinie wśród poprzednich klientów. Jeśli po wykonaniu tych kroków nadal nie jesteś pewny czy sklep jest prawdziwy, to z niego nie korzystaj. Zamiast takiego sklepu, lepiej użyj innego, który jest sprawdzony i masz co do niego pewność, nawet jeśli cena produktu, którego szukasz nie jest aż tak atrakcyjna.

Uchroń się przed oszustami internetowymi i kupuj tylko w zaufanych sklepach i serwisach aukcyjnych.

Bezpieczny komputer

Robienie zakupów tylko w bezpiecznych sklepach, to dobra praktyka, ale nie uchroni nas w zupełności przed próbami kradzieży danych lub pieniędzy. Musimy zapewnić, aby komputer, który wykorzystujemy do robienia zakupów online był bezpieczny. Płacąc za zakupy w Internecie przy użyciu komputera z wirusem, każda nasza transakcja i wszystko co napiszemy na klawiaturze może być przejęte i zmienione przez cyberprzestępcę, np. możemy stracić dane logowania do serwisów bankowych, kont email i innych ważnych usług. Upewnij się w 100%, że komputer, którego używasz nie jest zainfekowany i jest podłączony do zaufanej sieci. Miej przynajmniej zainstalowany system antywirusowy z aktualną bazą szczepionek oraz zaktualizowany cały system operacyjny i wszystkie aplikacje.

Jeśli masz dzieci, rozważ aby używały one oddzielnego komputera i nie korzystały z tego, którego Ty używasz na co dzień. Głównym powodem takiego podejścia jest to, że dzieci znacznie łatwiej mogą zarazić komputer złośliwym oprogramowaniem, głównie ze względu na nieuwagę. Używając oddzielnego komputera do transakcji bankowych, dokonywania opłat i zakupów w sieci minimalizujesz ryzyko infekcji wirusem i kradzieży Twoich danych lub środków. Jeśli użycie dwóch komputerów nie jest możliwe, upewnij się, że dzieci pracują na koncie z ograniczonymi uprawnieniami.

Karta kredytowa

Bądź ostrożny przy korzystaniu ze swojej karty kredytowej. Oznacza to, że powinieneś przeglądać miesięczne wyciągi z płatności, które z jej użyciem realizowałeś, aby szybko wykryć podejrzane transakcje. Niektóre z banków dają możliwość włączenia powiadomień SMS albo email dla każdej

Bezpieczne zakupy w sieci

realizowanej płatności pod warunkiem, że przekracza ona pewną wartość - zalecamy uruchomienie takiej usługi, aby być natychmiast powiadamianym o wszelkich zmianach na saldzie karty. Jeśli podejrzewasz, że któreś z transakcji nie były dokonane przez Ciebie, lub nie otrzymałeś zamówionego towaru pomimo prób kontaktu ze sprzedającym, jak najszybciej skontaktuj się ze swoim bankiem, wyjaśnij sytuację i poproś, aby skradzione środki zostały Ci zwrócone. W przypadku, gdy podawałeś dane karty kredytowej na stronie internetowej, która była fałszywym sklepem, zablokuj kartę i poproś bank o wydanie nowej. Aby uchronić się przed kradzieżą numeru karty kredytowej, rozważ korzystanie z serwisów pośredniczących w płatnościach, takich jak PayPal albo PayU. Dane Twojej karty musisz wtedy podać tylko na stronie zaufanego serwisu pośredniczącego, a nie w sklepie bezpośrednio. Sprawdź w swoim banku lub firmie, która wydała Ci kartę, jakie usługi związane z bezpieczeństwem płatności są przez nią zapewniane.

Dowiedz się więcej

Zasubskrybuj comiesięczny Biuletyn Bezpieczeństwa Komputerowego – SANS OUCH! Zdobądź dostęp do archiwów i poznaj rozwiązania SANS dotyczące bezpieczeństwa komputerowego i osobowego. Odwiedź http://www.securingthehuman.org i dowiedz się więcej.

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

Źródła

mBank - Bezpieczne zakupy:
http://www.mbank.pl/pomoc/info/bezpieczenstwo/bezpieczne-zakupy.html
NG - Bezpieczne zakupy:
http://www.ingbank.pl/indywidualni/karty/karty-platnicze/bezpieczne-zakupy-w-internecie
eCard- Bezpieczne zakupy:
http://www.ecard.pl/wybor-bezpiecznego-sklepu.htm
Chip - Bezpieczne płatności:
http://www.chip.pl/artykuly/porady/2013/08/bezpieczne-platnosci-internetowe-i-mobilne

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Polski przekład (NASK/CERT Polska): Katarzyna Gorzelak, Paweł Jacewicz, Łukasz Siewierski