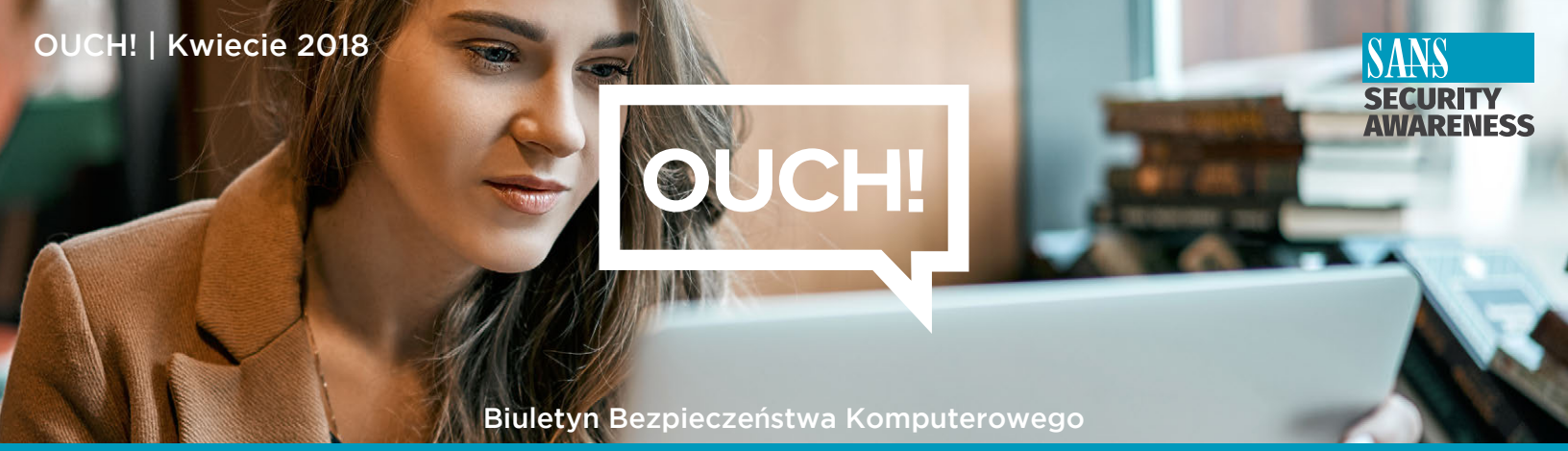

Biuletyn Bezpieczeństwa Komputerowego

Powstrzymać phishing

Wstęp

Email oraz serwisy takie jak Skype, Twitter czy Snapchat stanowią obecnie jeden z podstawowych sposobów komunikacji nie tylko w życiu prywatnym, ale również w pracy. Ponieważ społeczeństwo obecnie w tak dużej mierze opiera swoją komunikację na wiadomościach elektronicznych, stały się one jednym z podstawowych wektorów ataku wykorzystywanych przez przestępców. Zazwyczaj wykorzystywana jest metoda ataku nazwana phishingiem. W tym wydaniu opiszemy w jaki sposób w odpowiednim momencie zorientować się, że jesteśmy atakowani oraz nie stać się ofiarą niezależnie czy fałszywą wiadomość otrzymamy służbowo czy prywatnie.

Czym jest phishing

Phishing to typ ataku, w którym przestępcy używając specjalnie spreparowanych wiadomości chcą wprowadzić ofiarę w błąd i nakłonić do wykonania czynności, której nie powinna wykonać jak na przykład kliknięcie w złośliwy link, podanie hasła na niezaufanej stronie czy otwarcia zainfekowanego załącznika maila. Atakujący często starają się wykorzystywać fałszywe informacje w taki sposób by wzbudzić w ofierze emocje czy poczucie potrzeby podjęcia natychmiastowego działania lub zaciekawienia. W wiadomościach mogą podszywać się pod znajomego, którego dobrze znasz czy firmę, z której usług regularnie korzystasz. Przestępcy potrafią podrobić logo oraz wysłać wiadomość z adresu o łudząco podobnej nazwie. Tego typu kampanie wysyłane są zazwyczaj na masową skalę. Im więcej osób otrzyma wiadomość tym więcej ofiar prawdopodobnie "połknie haczyk".

Sposoby zabezpieczania się

W większości przypadków, otwarcie oraz odczytanie wiadomości nie prowadzi jeszcze do niczego złego. Aby phishing był skuteczny atakujący muszą nakłonić ofiarę do wykonania pewnej czynności. Na szczęście istnieją przesłanki mogące pomóc w odpowiednio wczesnym wykryciu ataku. Poniżej prezentujemy kilka z nich:

- Wiadomość wywołuje poczucie u odbiorcy potrzeby podjęcia natychmiastowego działania gdyż w innym wypadku wydarzy się coś złego. Za pomocą tej znanej metody atakujący chce sprowokować ofiarę do wykonania nieprzemyslanych działań.
- Atakujący próbuje nakłonić odbiorcę do ominięcia lub zignorowania procedur firmy.
- Treść wiadomości sprawia wrażenie czegoś zbyt pięknego, żeby było prawdziwe jak na przykład wygrana w dużej loterii.

- Bądź podejrzliwy w stosunku do wiadomości adresowanych w sposób ogólny, jak na przykład “Szanowny Kliencie”.
- Wiadomość zawiera prośbę o podanie wrażliwych informacji takich jak numer karty płatniczej, hasła lub innych informacji, do których prawdziwy nadawca powinien już mieć dostęp.
- Nadawca twierdzi, że jest z dużej organizacji, ale mail zawiera dużo błędów lub jest wysłany z ogólnodostępnych adresów @gmail.com, @wp.pl, lub @hotmail.com.
- Otrzymana wiadomość jest od znajomego, ale jej ton lub zastosowane zwroty nie pasują do tej osoby. Jeśli masz podejrzenia, zadzwoń do nadawcy czy się z Tobą kontaktował. Przestępcy mogą bardzo łatwo podrobić e-mail od przyjaciela bądź kolegi z pracy.

Zdrowy rozsądek to podstawowa linia obrony. Jeśli mail lub wiadomość wydaje się być podejrzana lub jej treść wskazuje na coś nieprawdopodobnego, to może być próba ataku phishingowego.

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

Tonia Dudley od 2011 roku opracowuje oraz prowadzi szkolenia z zakresu zwiększania świadomości zagrożeń bezpieczeństwa. W mediach społecznościowych można ją znaleźć pod adresem www.linkedin.com/in/toniadudley.

Przydatne linki

Inżynieria Społeczna:	https://www.sans.org/u/Cb1
O tym, jak pomóc innym zabezpieczyć się:	https://www.sans.org/u/Cb6
Email – kilka prostych porad:	https://www.sans.org/u/Cbg
CEO Fraud:	https://www.sans.org/u/Cbl
Archiwum biuletynów OUCH!:	https://www.sans.org/u/Cbq

Licencja

Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Polski przekład (NASK/CERT Polska): Sebastian Kondraszuk, Michał Strzelczyk, Jacek Sikorski