Dekalog bezpieczeństwa w Internecie

mBank.pl

Zabezpieczenia systemu CompanyNet

Ostatnie lata uczyniły Internet jednym z najpoważniejszych źródeł niebezpieczeństw dla przedsiębiorców. Wpływa na to zarówno powszechność dostępu do tego medium, jak i przenoszenie się do niego wielu codziennych czynności, takich jak kontakt z bliskimi, zakupy i transakcje. Wirusy, próby oszustw, czy tzw. złośliwe oprogramowanie, mogą w znaczący sposób wpłynąć na funkcjonowanie przedsiębiorstwa. Zadaniem Internetu jest ułatwienie nam życia, niemniej warto zapoznać się z zagrożeniami, jakie z niego płyną i zrobić wszystko, by uchronić przed nimi swoją firmę.

1 Zapoznaj się z zabezpieczeniami stosowanymi w serwisie mBank CompanyNet

Zawsze bezwzględnie stosuj się do zasad bezpieczeństwa opublikowanych na portalu mBanku. W przypadku pojawienia się jakichkolwiek nieprawidłowości, czy wątpliwości, natychmiast skontaktuj się ze wsparciem użytkowników systemu CompanyNet.

2 Loguj się do systemu CompanyNet korzystając wyłącznie z zaufanych i znanych Ci komputerów

Nie loguj się do systemu CompanyNet z komputerów znajdujących się poza siecią firmową.

3 Na bieżąco aktualizuj program antywirusowy, system operacyjny i istotne dla jego funkcjonowania aplikacje (przeglądarki Internetowe, etc.), cyklicznie skanuj komputer programem antywirusowym

Hakerzy stale szukają luk w oprogramowaniu, które są następnie wykorzystywane do przestępstw internetowych. Producenci systemów operacyjnych

i aplikacji publikują stosowne „łaty”, których celem jest usuwanie podatności na ataki przeprowadzane za pośrednictwem znalezionych luk. Działanie monitora antywirusowego może być słabsze niż skanera włączanego na żądanie dlatego też systematycznie skanuj komputer programem antywirusowym.

4 Niezwłocznie zgłoś do Banku nietypowe zachowanie systemu CompanyNet

W przypadku zaobserwowania nietypowego zachowania systemu, (np. wielokrotne błędne logowanie, dodatkowe pola do wprowadzenia haseł lub błędy przy autoryzacji płatności), niezwłocznie wstrzymaj się od dalszej pracy na urządzeniu, na którym występują objawy sugerujące działanie wirusa. Takie zachowanie systemu należy niezwłocznie zgłosić do Contact Center – wsparcia użytkowników systemu bankowości internetowej.

5 Zwracaj uwagę na numer rachunku kontrahenta

Podczas autoryzacji zleceń zweryfikuj numer rachunku kontrahenta. Istnieją wirusy, które podmieniają rachunek kontrahenta w pamięci przeglądarki .

6 Potwierdzaj w bezpieczny sposób zmianę numeru rachunku kontrahenta

Jeśli Twój kontrahent lub przełożony przekazał Ci mailowo lub telefonicznie informację o zmianie numeru rachunku, dodatkowo potwierdź to np. telefonicznie lub osobiście, aby upewnić się że informacja nie została sfałszowana.

7 Nie otwieraj wiadomości i znajdujących się w nich załączników nieznanego pochodzenia

Takie załączniki mogą zawierać wirusy lub inne szkodliwe oprogramowanie trudne do wykrycia przez programy antywirusowe.

8 Unikaj stron zachęcających do obejrzenia bardzo atrakcyjnych treści lub zawierających atrakcyjne okazje

Strony zawierające programy typu „freeware" również mogą być bardzo niebezpieczne, ponieważ hakerzy bardzo często uzupełniają je o złośliwy kod.

9 Nie otwieraj strony systemu CompanyNet za pośrednictwem linków znajdujących się w przychodzących do Ciebie mailach

Do logowania używaj tylko adresu systemu na portalu mBanku lub wchodź bezpośrednio na adres https://CompanyNet.mBank.pl.

10 Nigdy nie udostępniaj osobom trzecim swojego identyfikatora, aliasu ani tokena

Nadawany przez mBank identyfikator i tworzony przez użytkownika systemu CompanyNet alias są poufne. Zgodnie z postanowieniami umowy klient, a w rezultacie ich posiadacz, odpowiada za zachowanie poufności tych metod uwierzytelnienia.

Dzięki czemu nasze systemy mogą być bezpieczniejsze?

FireWall

Zapora sieciowa (ang. firewall – zapora ogniowa, ściana ognia) – jest jednym ze sposobów zabezpieczania komputerów, sieci i serwerów przed intruzami. Firewall może być zarówno sprzętem komputerowym ze specjalnym oprogramowaniem, bądź samym oprogramowaniem blokującym dostęp do naszych zasobów niepowołanym osobom lub programom. Jeszcze kilka lat temu oprogramowanie spełniające rolę firewalla było dostępne i dedykowane właśnie dla ważnych serwerów lub przy dużych sieciach. Jednak, wraz z ogromnym tempem wzrostu technologicznego, firewall staje się nieodzownym oprogramowaniem każdego domowego komputera podłączonego do sieci lokalnej LAN lub Internetu. Zapora na domowym komputerze sprawdza cały ruch sieciowy wchodzący i wychodzący, ogranicza i zabrania dostępu w obydwie strony nieznanym programom lub użytkownikom.

Programy antywirusowe

To oprogramowanie, którego zadaniem jest wykrywanie, zabezpieczanie, zwalczanie, usuwanie i naprawianie szkód spowodowanych wirusami. Jeśli uruchamiana aplikacja zawiera szkodliwe oprogramowanie, program wykonuje odpowiedni ruch, który wyklucza wirusa i pozwala na dostęp do uruchamianego programu.
Ważną funkcją każdego antywirusa jest odpowiednio częsta aktualizacja definicji wirusów zawartych w programie. Pozwala mu to „być na bieżąco" w świecie wirusów.
Dzięki uaktualnianym definicjom, program zbiera informacje o najnowszych wirusach i dostaje instrukcje, które pozwalają mu je zwalczać i naprawiać. Szanujące się firmy produkujące oprogramowanie antywirusowe w swoich produktach stosują codzienną aktualizację definicji wirusów.

Programy antyspamowe

To rodzaj oprogramowania służącego do blokowania niechcianej korespondencji przesyłanej drogą elektroniczną. Programy filtrują wiadomości i wykorzystują tak zwane czarne listy adresów i domen używanych przez spamerów. Większość tego typu oprogramowania posiada możliwość ustawiania własnych reguł, które możemy modyfikować i określać (np. słowa-klucze, występujące w materiałach reklamowych), blokując tym samym naszą skrzynkę pocztową na wiadomości zawierające te słowa w tytule przesyłki. Jednak programy te nie są bezbłędne i potrafią niekiedy zablokować korespondencję, która powinna być dostarczona.

Najczęściej spotykane zagrożenia w Internecie

Coraz częściej media donoszą, że hakerzy podszywają się pod kontrahenta lub przełożonych osób pracujących w systemach bankowych. Używając ataków socjotechnicznych, starają się doprowadzić do realizacji nieplanowanej lub zaplanowanej płatności na fałszywy, podany mailem lub telefonicznie numeru rachunku kontrahenta. Każda operacja zmiany numeru rachunku powinna być dodatkowo potwierdzona w inny sposób niż dotarła pierwotna wiadomość.
Inne, często spotykane zagrożenia to podstępne pozyskanie poufnej informacji osobistej, jak hasła, identyfikatora i aliasu użytkowników, czy szczegółów związanych z kartą kredytową. Jest to rodzaj ataku opartego na inżynierii społecznej. Dzisiaj przestępcy sieciowi wykorzystują techniki phishingu w celach zarobkowych. Popularnym celem są banki czy aukcje Internetowe. Phisher wysyła zazwyczaj spam do wielkiej liczby potencjalnych ofiar, kierując je na stronę, która udaje rzeczywisty bank Internetowy, tymczasem przechwytując wpisywane tam przez ofiary ataku informacje. Typowym sposobem jest informacja o rzekomej dezaktywacji konta i konieczności aktywacji poprzez podanie poufnych informacji. Częstym sposobem jest również imitacja strony banku Internetowego, na której użytkownik wpisuje wszystkie potrzebne informacje do poprawnego zalogowania się. Logowanie jednak się nie odbywa, a dane wpisane przez użytkownika uzyskuje phisher.

Spam

Spam to niechciana korespondencja rozsyłana drogą elektroniczną w postaci poczty e-mail. Zazwyczaj jest wysyłany masowo. Istotą spamu jest rozesłanie dużej liczby informacji komercyjnych o jednakowej treści do nieznanych sobie osób. Treść wiadomości nie ma znaczenia. Spam można porównać do ulotek zostawianych pod drzwiami naszych mieszkań, czy dołączanych do naszej korespondencji. W większości przypadków spam służy do celów komercyjnych, w korespondencji elektronicznej namawia nas na kupno danych artykułów lub wabi wygraną wycieczką. Czasem jednak spam jest narzędziem ataku na nas poprzez próby wydobycia poufnych informacji podszywając się pod bank lub inną instytucję lub próbą skłonienia nas do zainstalowania programów zawierających wirusy i programy szpiegujące.

Wirusy

Wirus komputerowy to powielający się segment wykonywalnego kodu, umieszczony w innym programie lub sprzężony z nim. Wirus nie może działać sam, potrzebuje nosiciela w postaci programu komputerowego. Po uruchomieniu tego programu zazwyczaj pierwszy uruchamia się złośliwy kod wirusa, a następnie właściwy program.

Po skutecznej infekcji dalsze działanie zależy od określonego typu wirusa i obejmuje

- wyłudzenie danych umożliwiających realizację płatności w bankowości Internetowej
- replikację jedynie w zainfekowanym systemie
- infekcję dalszych plików podczas ich uruchamiania lub tworzenia
- kasowanie lub uszkadzanie danych w systemach i plikach
- marnowanie zasobów systemowych bez powodowania szkód

Ze względu na rodzaje wirusów można je podzielić na

- dyskowe – infekują sektory startowe dyskietek i dysków twardych
- plikowe – infekują pliki wykonywalne danego systemu operacyjnego
- wirusy BIOS-owe – niszczą BIOS komputera (oprogramowanie odpowiadające za poprawna konfigurację i start systemu)
- makrowirusy – atakują przez pliki niewykonywalne, np. pliki dokumentu Word lub Excel, infekcja odbywa się poprzez makra zawarte w tych dokumentach
- wirusy komórkowe – coraz częściej spotykane, zaczynają stanowić istotne zagrożenie w związku z rozwojem oprogramowania dla telefonów

mBank S.A. ul. Senatorska 18, 00-950 Warszawa
tel. 22 829 00 00, fax 22 829 00 33
msp-korporacje@mBank.pl