WSTĘP

System bankowości elektronicznej zapewnia dostęp do rachunków przez Internet, 24 godziny na dobę, 7 dni w tygodniu z każdego miejsca na terenie krajów Unii Europejskiej, Szwajcarii, Stanów Zjednoczonych oraz Kanady, umożliwia komplementarną obsługę Państwa instytucji bez konieczności wizyty w Oddziale Banku Gospodarstwa Krajowego.

Ze względów bezpieczeństwa i w celu zabezpieczenia przed nieuprawnionym dostępem do Państwa rachunku, bankowość elektroniczna poza zakresem krajów wyżej wymienionych zostanie czasowo udostępniona po uprzednim wcześniejszym zgłoszeniu tej potrzeby za pośrednictwem BGK Linia, gdzie uzyskacie Państwo informacje odnośnie warunków jej udostępnienia.

BEZPIECZNE KORZYSTANIE Z SYSTEMÓW BGK

Ostatnie lata uczyniły Internet jednym z najpoważniejszych źródeł niebezpieczeństw. Wpływa na to jego powszechna dostępność, jak i przenoszenie do Internetu wielu codziennych czynności oraz operacji gospodarczych, takich jak np. transakcje finansowe dokonywane z wykorzystaniem bankowości elektronicznej. Infekcja infrastruktury teleinformatycznej złośliwym oprogramowaniem i próby oszustw mogą w znaczący sposób wpłynąć na sposób funkcjonowania firmy. Aby korzystanie z Internetu i bankowości elektronicznej było bezpieczne, należy konieczne zapoznać się z potencjalnymi zagrożeniami i zrobić wszystko, aby się przed nimi chronić.

Oferowane przez BGK systemy spełniają najwyższe wymagania w zakresie bezpieczeństwa. Jednocześnie należy pamiętać, iż słabym ogniwem może okazać się człowiek oraz każde środowisko teleinformatyczne, które znajduje się poza kontrolą banku. Każdy użytkownik Internetu dba samodzielnie o bezpieczeństwo własnego sprzętu teleinformatycznego oraz ma wpływ na bezpieczeństwo swojego konta w systemie BGK – żadne zabezpieczenia techniczne nie pomogą, jeśli użytkownicy systemów teleinformatycznych nie będą stosować się do podstawowych zasad bezpieczeństwa. Konsekwentne stosowanie tych zasad pozwala uniknąć potencjalnych niebezpieczeństw płynących z Internetu.

BGK oferuje usługi bankowości elektronicznej klientom instytucjonalnym – w tym instytucjom i organom państwowym, samorządom, przedsiębiorcom oraz bankom. Jesteście Państwo gronem klientów, którzy powinni stosować się – ze wsparciem swoich wewnętrznych lub zewnętrznych służb informatycznych – do restrykcyjnych zasad bezpieczeństwa.

Wśród generalnych zasad bezpieczeństwa teleinformatycznego klienta instytucjonalnego powinny się znaleźć m.in.:

1. Regularne przeprowadzanie szkoleń w obszarze cyberbezpieczeństwa, prowadzenie akcji uświadamiających oraz informowanie pracowników o aktualnych zagrożeniach związanych z urządzeniami teleinformatycznymi, w tym o zagrożeniach związanych z korzystaniem z Internetu czy użytkowaniem urządzeń mobilnych itp.
2. Systematyczne zaznajamianie wszystkich użytkowników bankowości elektronicznej BGK, osoby ich nadzorujące oraz kadrę zarządzającą z bieżącymi komunikatami na temat bezpieczeństwa znajdującymi się na stronie banku – www.bgk.pl.
3. Zalecane jest, aby – tam, gdzie jest to możliwe – schematy akceptacji wymuszały posiadanie dwóch osób akceptujących oraz aby wprowadzający nie mógł sam akceptować własnych dyspozycji.
4. Stosowanie dla służbowych urządzeń mobilnych (np. smartfony, tablety) takiego samego poziomu ochrony jak dla komputerów stacjonarnych; używanie oprogramowania bezpieczeństwa, które służy do wykrywania i usuwania szkodliwego i szpiegującego oprogramowania oraz zabezpiecza poufność i zapobiega kradzieży danych.
5. Powierzanie dokonywania konfiguracji urządzeń teleinformatycznych, w tym sieci i urządzeń sieciowych, wyłącznie specjalistom z obszaru IT.
6. Stosowanie uznanych branżowych standardów, norm i najlepszych praktyk w zakresie bezpieczeństwa teleinformatycznego i bezpieczeństwa informacji.
7. Dokonywanie systematycznych audytów bezpieczeństwa infrastruktury teleinformatycznej.
8. Posiadanie procedury postępowania w sytuacji wystąpienia incydentu bezpieczeństwa teleinformatycznego przykładowo polegającego na złamaniu zabezpieczeń systemu teleinformatycznego, podejrzeniu infekcji złośliwym oprogramowaniem, podejrzeniu kradzieży danych autoryzacyjnych do systemu BGK itp.

ZASADY BEZPIECZNEGO KORZYSTANIA Z SYSTEMU BANKOWOŚCI ELEKTRONICZNEJ

Poniżej znajdują się obowiązujące Państwa (oraz upoważnionych przez Państwa użytkowników systemu BGK) podstawowe zasady bezpiecznego korzystania z systemu bankowości elektronicznej BGK.

I. Zabezpieczenie fizyczne

1. Do systemu BGK loguj się wyłącznie ze służbowych/firmowych komputerów.
2. Nie pozostawiaj zalogowanego konta w systemie BGK bez nadzoru.
3. Po skończonej pracy zawsze wyloguj się zgodnie z procedurą banku.

4. Jeśli korzystasz z certyfikatu kwalifikowanego – niezwłocznie po zakończeniu akceptacji dyspozycji wyjmij go z czytnika/portu USB.
5. Zabezpiecz narzędzia autoryzacyjne (certyfikat, token) przed niepowołanym dostępem.
6. Nigdy nie udostępniaj nikomu danych służących do logowania do systemu BGK.

II. Zabezpieczenie oprogramowania

1. Używaj wyłącznie legalnego oprogramowania pochodzącego z zaufanego źródła. Dotyczy to systemu operacyjnego, przeglądarki internetowej oraz wszelkiego innego oprogramowania używanego w systemie teleinformatycznym, włączając urządzenia mobilne.
2. Używaj i na bieżąco aktualizuj program antywirusowy renomowanego producenta oraz rozwiązania zabezpieczające przed złośliwym oprogramowaniem (m.in. typu spyware, adware), a także zaporę sieciową (ang. *firewall*). Cyklicznie skanuj programem antywirusowym każde urządzenie teleinformatyczne.
3. Regularnie aktualizuj całe swoje oprogramowanie, w tym system operacyjny i przeglądarkę, poprzez wgrywanie aktualnych poprawek (ang. *patch*) publikowanych na stronach producentów danego oprogramowania.
4. Świadomie wybierz przeglądarkę internetową i na bieżąco przeprowadzaj jej konfigurację bezpieczeństwa. Używaj najnowszej wersji przeglądarki internetowej. Pamiętaj, aby systematycznie usuwać pliki tymczasowe zapisywane w podręcznej pamięci przeglądarki, aby zapewnić jej poprawne funkcjonowanie. Wyłącz wszelkie zbędne wtyczki (*plug-in*) w przeglądarce.
5. Przed instalacją jakiegokolwiek oprogramowania dodatkowego związanego bezpośrednio z systemem BGK zwróć się z pytaniem do Infolinii BGK.
6. W przypadku podejrzenia infekcji komputera powiadom bezzwłocznie swoje służby informatyczne. Symptomami zainfekowania komputera są zwykle: znaczne spowolnienie działania systemu, zmiany w działaniu przeglądarki internetowej, problemy z działaniem niektórych programów.

III. Zabezpieczenie sieciowe

1. Systemy BGK dostępne przez przeglądarkę internetową posiadają zabezpieczenia uniemożliwiające pracę, gdy adresy IP przyznawane są dynamicznie i zmieniają się w trakcie trwania sesji. W takiej sytuacji następuje automatyczne wylogowanie w ramach procedury bezpieczeństwa przed potencjalnymi atakami.
2. Bank nie rekomenduje połączenia z systemem BGK poprzez inne niż zaufane służbowe/firmowe sieci, w tym bezprzewodowe (np. dostępne w hotelach, na lotniskach, sieci innych kontrahentów itp.). Jeśli jednak jest taka konieczność, zawsze łącz się poprzez VPN.
3. Koniecznie zdefiniuj adresy IP, tak aby ograniczyć możliwość logowania do systemu BGK z innych adresów. Możesz to zrobić, kontaktując się z swoim doradcą.

4. Bank rekomenduje, aby komputery, na których korzystasz z systemu BGK, nie służyły do innej aktywności w Internecie, np. przeglądania stron WWW, itp.

IV. Zabezpieczenie socjotechniczne

1. Nie otwieraj strony do logowania bankowości elektronicznej BGK z linków (np. otrzymanych mailem, SMS-em). Wpisuj ręcznie adres strony lub loguj się poprzez www.bgk.pl.
2. Nie kopiuj numerów rachunków bankowych do przelewów (kopiuj – wklej). Wpisuj je ręcznie i dokładnie weryfikuj.
3. Nie ufaj nadawcy nietypowych wiadomości e-mail (konieczność podjęcia natychmiastowego działania, realizacji zobowiązania finansowego, otwarcia załącznika zabezpieczonego hasłem itp.). Oszuści mają możliwość spreparowania wiadomości tak, aby sprawiała wrażenie, że wysłała ją osoba lub instytucja, której ufasz. W przypadku podejrzeń weryfikuj niezależnym kanałem fakt jej wysłania przez nadawcę, innym niż numer telefonu podany w takiej wiadomości.
4. Nie otwieraj wiadomości (oraz załączników) otrzymanych pocztą elektroniczną od nieznanych nadawców.
5. Nie otwieraj linków/hiperłączy bezpośrednio z otrzymanego e-maila, komunikatora internetowego, SMS itp. Nigdy nie uruchamiaj w ten sposób programów komputerowych. Zwracaj uwagę na wiarygodność otrzymywanych poprzez e-mail komunikatów, ponieważ mogą zawierać linki do fałszywej strony systemu BGK; zalogowanie na takiej stronie powoduje udostępnienie loginu i hasła oszustowi.
6. Nie zapisuj loginu ani haseł dostępu na papierze lub w plikach tekstowych – narażasz się na ich przechwycenie.
7. Nie przesyłaj e-mailem czy SMS-em żadnych danych osobistych, haseł, loginów, numerów kart kredytowych itp.
8. Pamiętaj, że Bank nie weryfikuje poprawności Twoich danych autoryzacyjnych poprzez e-mail czy wiadomości tekstowe w telefonie komórkowym, dlatego też nigdy nie odpowiadaj na tego typu e-maile i wiadomości.
9. Bank nigdy nie poprosi Cię o podanie danych autoryzacyjnych: hasła, numeru PIN lub kodu jednorazowego.
10. W trakcie korzystania z wielu stron internetowych równocześnie sprawdzaj, czy żadna ze stron (kart w przeglądarce) nie została podmieniona na inną stronę. Niezauważenie podmiany strony na stronę oszusta może przyczynić się do nieumyślnego zalogowania do podstawionej strony systemu BGK i udostępnienia oszustowi danych do logowania.
11. Przed wysłaniem/autoryzacją przelewu zawsze upewnij się, czy wprowadzony numer rachunku odbiorcy nie został podmieniony przez złośliwe oprogramowanie. Sprawdź numer rachunku z dokumentem źródłowym.
12. Na bieżąco przeglądaj historię rachunku i operacji.
13. Cyklicznie sprawdzaj, czy numery rachunków w zdefiniowanych kontrahentach nie uległy podmianie.

14. Niezwłoczne zgłaszaj do banku wszelkie podejrzane i nietypowe zachowania systemu BGK, podejrzenia infekcji komputerowej oraz nieautoryzowane zmiany danych w systemie BGK (przelewów, kontrahentów).

Szczegółowe zasady dotyczące prawidłowego korzystania i dokonywania operacji w systemach BGK zawiera instrukcja użytkownika.

Informacje i ostrzeżenia bezpieczeństwa zamieszczone na stronie internetowej www.bgk.pl należy śledzić na bieżąco.

ZGŁASZANIE PROBLEMÓW DOTYCZĄCYCH BEZPIECZEŃSTWA I WSPÓŁPRACA Z BANKIEM

Użytkownicy systemu bgk24 powinni zgłaszać problemy dotyczące bezpieczeństwa oraz zdarzenia budzące wątpliwości w następujących formach:

- Telefonicznie na infolinię BGK pod numerami telefonów: 801 598 888 lub 22 475 8888
- Poprzez wysłanie wiadomości e-mail na adres: bgk24@bgk.pl.
- Poprzez zarejestrowanie informacji o zdarzeniu poprzez formularz kontaktowy na stronie www.bgk.pl.

W każdej niepokojącej sytuacji, a w szczególności w sytuacji wykrycia przez system antywirusowy złośliwego oprogramowania, istnieje podejrzenie, że mogło dojść do wycieku danych do logowania, tj. loginu i hasła. Wówczas należy natychmiast skontaktować się z bankiem. W przypadku konieczności zablokowania dostępu użytkownikom, których dane do logowania wyciekły, wymagane jest złożenie wniosku o ponowne nadanie dostępu dla wskazanych użytkowników.

W sytuacji wykrycia złośliwego oprogramowania, informacji z banku o podejrzanych operacjach oraz wszelkich budzących wątpliwości zdarzeniach w systemie IT lub systemie BGK należy niezwłocznie wykonać analizę mającą na celu:

- przejrzenie historii przelewów, weryfikację wszystkich aktualnie widocznych w systemie bankowości elektronicznej przelewów – zarówno już zrealizowanych, jak i oczekujących na akceptację – czy nie zostały zmodyfikowane przez wirus lub osobę nieuprawnioną; w szczególności poprawność numeru rachunku bankowego beneficjenta przelewu;
- weryfikację danych zdefiniowanych kontrahentów – w szczególności ich numery rachunków, czy nie został zmodyfikowany przez wirus lub osobę nieuprawnioną.

W przypadku wykrycia nieuprawnionego wprowadzenia, edycji, skasowania przelewu lub edycji kontrahenta o zdarzeniu należy natychmiast poinformować bank oraz nie dopuścić do podpisania/autoryzacji podejrzanego przelewu lub użycia zmodyfikowanych danych kontrahenta w nowych przelewach. W sytuacji, kiedy zostanie

wykryte wprowadzenie nieuprawnionego przelewu lub nieuprawniona edycja przelewu, a przelew został już zaakceptowany i wysłany, należy o tym fakcie natychmiast poinformować bank oraz złożyć zawiadomienie o podejrzeniu popełnienia przestępstwa do organów ścigania.

W przypadku podejrzenia ataku na system teleinformatyczny lub próby manipulacji w systemie BGK, urządzenia teleinformatyczne, które mogły stać się przedmiotem ataku, powinny zostać odłączone od sieci (nie należy usuwać danych ani skanować zainfekowanego komputera; działania te mogą utrudnić lub uniemożliwić ewentualne wyjaśnienie zdarzenia przez organy ścigania). W takim przypadku zaleca się przeprowadzenie pogłębionej analizy bezpieczeństwa systemów teleinformatycznych przez wyspecjalizowane służby IT.

Zachęcamy do zapoznania się z informacjami na temat bezpieczeństwa przygotowanymi przez Związek Banków Polskich w zakładce „Dla Klientów – Bezpieczny Bank" http://zbp.pl/dla-konsumentow/bezpieczny-bank/aktualnosci oraz na stronie Komisji Nadzoru Finansowego:

- „Zadbaj o swoje bezpieczeństwo w sieci" http://www.knf.gov.pl/bezpieczenstwo_w_sieci.html
- „Poradnik klienta usług finansowych. Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną" https://www.knf.gov.pl/Images/Bezp_finansowe_tcm75-39005.pdf

Powyższe zasady należy traktować jako podstawowe zalecenia z zakresu bezpieczeństwa, a poniższe zagrożenia to jedynie przykłady, jakie bank przekazuje w ramach informacji – nie wyczerpują one tego obszernego tematu.

OPIS NAJCZĘŚCIEJ SPOTYKANYCH ZAGROŻEŃ

Kluczową kwestią jest zdanie sobie sprawy z tego, że obecnie każdy użytkownik Internetu jest narażony na cyberzagrożenia. Istotna jest również świadomość, iż metody działania przestępców wcale nie muszą być skomplikowane, a czynnikiem umożliwiającym większość kradzieży jest błąd człowieka i brak zachowania podstawowych zasad bezpieczeństwa.

Metody działania przestępców są różne, a systematyczne doniesienia o takich przypadkach są publikowane w mediach. Oszustwa skierowane na klientów bankowości elektronicznej ostatecznie mają na celu realizację płatności lub wypłatę z rachunku na rzecz przestępców (np. na rachunek w innym banku).

Przestępcy powszechnie wykorzystują socjotechnikę rozumianą jako zestaw metod mających na celu skłonienie do określonego działania, np. uzyskania informacji. Technika ta wykorzystuje umiejętności interpersonalne, zdolność do manipulowania ludźmi, co w połączeniu z wiedzą informatyczną daje szerokie

spektrum pozyskiwania wiedzy na temat użytkowników, ich systemów teleinformatycznych, sposobów pracy oraz posiadanych danych.

Aktualnie stosowane metody ataków są niejednokrotnie wykładnią kliku znanych – w tym opisanych poniżej – sposobów wyłudzania poufnych danych (np. loginu, hasła, kodu jednorazowego do autoryzacji w systemie bankowości elektronicznej) lub manipulacji (np. fałszywe faktury, podszywanie się pod przełożonych), a w konsekwencji umożliwiających skuteczne włamanie i wyprowadzenie środków finansowych. Poniżej opisano kilka z wielu stosowanych metod oszustwa.

1. Phishing

Metoda oszustwa, kiedy przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej. Może być realizowany poprzez nakłonienie potencjalnej ofiary do wejścia na fałszywą stronę internetową czy do logowania się do bankowości elektronicznej – adresem i wyglądem może łudząco przypominać prawdziwą stronę logowania. *Phishing* może być także próbą nakłonienia do podania poufnych danych logowania i autoryzacji operacji w wiadomości e-mail lub telefonicznie.

Ważne jest, aby zawsze w przeglądarce internetowej wpisywać ręcznie adres strony logowania do bankowości elektronicznej lub logować się poprzez www.bgk.pl (zakładka „Strefa logowania”). Zapisane w przeglądarce skróty do logowania lub klikanie w linki otrzymane w wiadomościach e-mail, komunikatorach internetowych, SMS-ach itp. są podatne na manipulacje, przez co mogą być również wykorzystywane przez przestępców.

Przestępcy, rozsyłając oszukańcze e-maile, stosują najrozmaitsze metody socjotechniczne, aby wzbudzić zaufanie, zainteresowanie lub niepokój, przykładowo:

- nadawcą jest powszechnie znany podmiot usług masowych (poczta, dostawca energii, operator telefoniczny itp.),
- wiadomość dotyczy szczególnie atrakcyjnej, ale ograniczonej czasowo oferty,
- wiadomość informuje o niezapłaconej fakturze,
- dotyczy rzekomo wysłanej wiadomości, która nie została dostarczona do adresata,
- dotyczy konieczności podania danych logowania do bankowości elektronicznej na skutek awarii tego systemu celem „weryfikacji ze względów bezpieczeństwa” lub „wzmocnienia zabezpieczeń procesu logowania” itp. Należy jednak pamiętać, że bank **nigdy** nie przesyła takich wiadomości.

Ważne jest także, aby – korzystając z urządzeń teleinformatycznych – wyrobić sobie nawyk krytycznego podejścia do wszelkiej niespodziewanej korespondencji (e-mail, SMS, rozmowy telefoniczne z nieznaną osobą itp.), jaka budzi podejrzenia bądź wymaga podjęcia pilnych działań. **Nie należy** otwierać załączników i klikać w

linki zawarte w takich wiadomościach; **nie należy** pobierać i uruchamiać samodzielnie oprogramowania z Internetu (należy zostawić to służbom IT); **nie należy** również podawać telefonicznie informacji służących do logowania ani żadnych innych wrażliwych danych.

2. Złośliwe oprogramowanie

Klikanie w niesprawdzone linki, otwieranie załączników do wiadomości e-mail, uruchamianie programów pobranych z Internetu czy wchodzenie na podejrzane strony internetowe np. nieopatrzone certyfikatem poufności grozi infekcją złośliwego oprogramowania (wirus komputerowy). W przypadku niektórych zagrożeń nawet renomowany i poprawnie skonfigurowany program antywirusowy nie uchroni przed instalacją wirusa w systemie teleinformatycznym. Taka infekcja jest możliwa **na skutek braku aktualizacji** – systemu operacyjnego lub innego używanego programu komputerowego – przez istnienie tzw. podatności oprogramowania, które nie zostały wyeliminowane poprzez jego aktualizację. Dlatego tak istotne jest korzystanie z najnowszych wersji oprogramowania.

Istnieje wiele rodzajów złośliwego oprogramowania, lecz ważne jest, aby zdawać sobie sprawę ze skutków jego działania po udanej infekcji:

- przesyłanie do przestępców danych, zapisanych lub wprowadzanych do urządzenia komputerowego, umożliwiających realizację płatności w bankowości elektronicznej,
- podmianę numeru rachunku bankowego beneficjenta przelewu w trakcie jego kopiowania metodą „kopiuj – wklej”,
- infekcję dalszych plików podczas ich uruchamiania lub tworzenia,
- replikację w zainfekowanym systemie,
- kasowanie lub uszkadzanie danych,
- szyfrowanie zawartości urządzenia komputerowego (np. w celu żądania okupu w zamian za podanie hasła do odszyfrowania),
- spowalnianie pracy urządzenia komputerowego.

Ostatnio wiele infekcji powoduje złośliwe oprogramowanie typu *ransomware/cryptolocker*. Zainfekowany w ten sposób komputer zostaje zaszyfrowany, a do jego odszyfrowania potrzebne jest znane tylko przestępcom hasło. W zamian za podanie hasła przestępcy żądają okupu – najczęściej w kryptowalucie (np. *bitcoin*). Przykładowe nazwy złośliwego oprogramowania typu *ransomware/cryptolocker*: Cerber, Locky, CryptXXX, CrypMIC, PCrypt, Petya, Mischa, Crypt0L0cker. Taka infekcja może powodować brak możliwości używania komputerów, a w sytuacji braku aktualnej kopii zapasowej systemu i danych może skutkować ich utratą.

3. Fałszywe faktury / podszywanie się pod przełożonych

Przestępcy potrafią z łatwością spreparować wiadomość e-mail lub SMS tak, aby wyglądała, że pochodzi nawet z prawidłowego adresu lub numeru telefonu przełożonego. Przed realizacją nietypowych poleceń skierowanych do nas w takich wiadomościach drogą elektroniczną, zawsze – osobiście lub innym niezależnym kanałem – należy weryfikować prawdziwość takich poleceń. Przydatne jest zgłębienie wiedzy w tym temacie poprzez wpisanie w wyszukiwarkę internetową hasła: „oszustwo na prezesa".

Wszelkie nowe płatności (np. pierwsza faktura od danego kontrahenta) lub zmiany numeru rachunku bankowego kontrahenta należy potwierdzić niezależnym kanałem. Ważne jest, aby nie był to kontakt poprzez odesłanie na adres nadawcy wiadomości, która informuje o nowym rachunku bankowym kontrahenta. Nie powinien to być również kontakt telefoniczny na numer wskazany w takiej wiadomości. Jeśli wiadomość pochodzi od oszusta, to zarówno adres nadawcy mógł zostać spreparowany, jak i numer telefonu kontrahenta w takiej wiadomości może być fałszywy.