

# czytaj Aktualności CitiService

Lipiec 2022 r. | wydanie nr 7

Serwisy na skróty:

Szybki kontakt z doradcą CitiService

 tel.: 801 24 84 24; 22 690 19 81

# Bezpieczeństwo: ransomware

System Protected

**Ransomware** to złośliwe oprogramowanie, które blokuje komputer i urządzenia mobilne lub szyfruje pliki elektroniczne, żądając zapłaty okupu za pomocą określonych metod płatności online (w ustalonym terminie) w celu uzyskania kontroli nad Twoimi danymi. Można je pobrać przez fałszywe aktualizacje aplikacji lub odwiedzając zainfekowane strony internetowe. Może być również dostarczone jako załącznik do wiadomości e-mail w spamie lub pobrane za pośrednictwem innego złośliwego oprogramowania (np. trojana). Takie oszustwo ma na celu generowanie ogromnych zysków dla zorganizowanych grup przestępczych.

**Aby zapobiegać skutkom oprogramowania ransomware lub by je skutecznie ograniczyć, zalecamy podjęcie następujących działań:**

- **REGULARNIE AKTUALIZUJ SWOJE OPROGRAMOWANIE**

Wiele infekcji złośliwym oprogramowaniem bierze się stąd, że przestępca wykorzystuje błędy w oprogramowaniu (przeglądarki internetowe, systemy operacyjne, wspólne narzędzia itp.). Aktualizowanie ich na bieżąco może pomóc ochronić urządzenia i pliki.

- **UŻYWAJ OPROGRAMOWANIA ANTYWIRUSOWEGO**

Zainstaluj i aktualizuj oprogramowanie antywirusowe i zapory na swoich urządzeniach. Oprogramowanie antywirusowe może pomóc chronić komputer przed najpopularniejszym złośliwym oprogramowaniem. Zawsze sprawdzaj pobrane pliki za pomocą oprogramowania antywirusowego.

- **PRZEGLĄDAJ I POBIERAJ OPROGRAMOWANIE TYLKO Z ZAUFANYCH STRON INTERNETOWYCH**

Korzystaj z oficjalnych źródeł i wiarygodnych stron internetowych. Aktualizuj swoje oprogramowanie najnowszymi wydaniem bezpieczeństwa. Zawsze używaj oficjalnej wersji oprogramowania.

- **REGULARNIE WYKONUJ KOPIĘ ZAPASOWĄ PRZECHOWYWANYCH DANYCH W TWOIM KOMPUTERZE**

Pełne kopie zapasowe danych pozwolą Ci zaoszczędzić czas i koszty w razie przywracania danych komputera. Nawet jeśli padniesz ofiarą ransomware, nadal będziesz mieć dostęp do swoich osobistych plików (zdjęć, list kontaktów itp.) z innego komputera. Wiele zaufanych rozwiązań pozwalających na wykonanie kopii zapasowych Twoich danych dostępnych jest w internecie za darmo.

- **ZAPYTAJ DOSTAWCĘ OPROGRAMOWANIA ANTYWIRUSOWEGO, JAK ODBLOKOWAĆ I USUNĄĆ INFEKCJE Z URZĄDZENIA**

Z wielu oficjalnych stron internetowych i blogów dowiesz się, jak bezpiecznie usunąć złośliwe oprogramowanie z urządzeń elektronicznych. Zawsze sprawdzaj na stronie [www.nomoreransom.org](http://www.nomoreransom.org), czy zostałeś zarażony jednym z wariantów oprogramowania ransomware, dla których istnieją narzędzia deszyfrujące. Są one dostępne bezpłatnie.

- **ZGŁOŚ SWÓJ PRZYPADEK**

Jeśli jesteś ofiarą oprogramowania ransomware, zgłoś to natychmiast do banku oraz na policję. Im więcej informacji dostarczysz władzom, tym skuteczniej utrudnisz życie organizacji przestępczej.

## PAMIĘTAJ:

- **NIE KLIKAJ W ZAŁĄCZNIKI, BANERY I LINKI BEZ ZNAJOMOŚCI ICH PRAWDZIWEGO POCHODZENIA**

Coś wygląda na nieszkodliwą reklamę? Miej świadomość, że kliknięcie w grafikę może przekierować Cię na stronę, z której pochodzi złośliwe oprogramowanie. To samo może się zdarzyć, gdy otworzysz załącznik w wiadomości e-mail otrzymanej z nieznanego źródła.

- **NIE INSTALUJ APLIKACJI MOBILNYCH OD NIEZNANYCH DOSTAWCÓW/ŹRÓDEŁ**

Aplikacje pobieraj tylko z oficjalnych i zaufanych zasobów. W ustawieniach na urządzeniu z Androidem zawsze miej wyłączonej opcje „Nieznane źródła”, a zaznaczoną - „Zweryfikuj aplikacje”.

- **NIE BIERZ WSZYSTKIEGO ZA PEWNIK**

Jeśli witryna ostrzega Cię o przestarzałym oprogramowaniu, sterowniku lub kodeku (programy, które szyfrują i dekodują Twoje dane) zainstalowanych na Twoim komputerze, pamiętaj o zasadzie ograniczonego zaufania. Przestępcom jest naprawdę łatwo wykonać fałszywe logo firmy i oprogramowania. Szybkie wyszukanie w sieci pomoże Ci potwierdzić, czy Twoje oprogramowanie jest naprawdę nieaktualne.

- **NIE INSTALUJ LUB NIE URUCHOMIAJ NIEZAUFANEGO LUB NIEZNANEGO OPROGRAMOWANIA**

Nie instaluj programów ani aplikacji na swoim komputerze, jeśli nie wiesz, skąd pochodzą. Niektóre elementy złośliwego oprogramowania instalują się w programach działających w tle, i próbują ukraść dane osobiste.

Wszelkie podejrzane sytuacje powinny być niezwłocznie zgłaszane do CitiService pod numer: **(22) 690 19 81** lub **801 24 84 24** albo pod adresem [citIService.polska@citi.com](mailto:citIService.polska@citi.com).

Doradcy są dostępni od poniedziałku do piątku w godz. 8:00-17:00. Poza tymi godzinami zgłoszenia należy kierować na adres e-mail: [alert.fraud@citi.com](mailto:alert.fraud@citi.com).

**POWRÓT >>**

# Karty Business: zmiana dokumentacji

Uprzejmie informujemy, że **zmianie ulega dokumentacja Kart Business.**

Zmiany mają na celu dostosowanie wniosków i formularzy do wprowadzonych nowych modułów samoobsługi w platformie CitiManager (aplikowanie online o kartę OLA i zarządzania online kartami OLM). Równocześnie redukujemy ilość dokumentów poprzez integrację osobnych formularzy dla Kart Kredytowych i Debetowych w jednym dokumencie dla Kart Business.

Zakres zmian obejmuje m.in:

- wprowadzenie definicji *Osoby upoważnionej do działania w imieniu Użytkownika oraz Administratora Programu* (w miejsce dotychczasowej definicji *Pełnomocnika*)
- wprowadzenie *Formularza Administratorów Programu Kart Business* (w miejsce *Karty Pełnomocników Programu Karta VISA Business* oraz *Karty Pełnomocników Programu Kart Debetowych VISA Business*) i **zaprzestanie zbierania wzorów** podpisów (wzory podpisów są ustalane w ramach otwierania rachunku bankowego)
- **usunięcie** z *Wniosku o wydanie Karty Business* **pola z adresem zamieszkania** i zaprzestanie zbierania oraz aktualizacji danych w tym zakresie
- usunięcie *Wniosku o Wydanie Karty Business* jako załącznika do *Umowy o Wydanie Kart Business* oraz *Obsługę Operacji dokonywanych przy Ich Użyciu* (wnioski o wydanie Karty Business będą standardowo składane poprzez platformę CitiManager).

**Od dnia 15 lipca 2022 r. prosimy o korzystanie z formularzy opatrzonych sygnaturą STANDARD 062022.** Wnioski złożone na starych formularzach będą obsługiwane tylko do dnia 30 września 2022 r. Wyjątkiem jest Wniosek o wydanie Karty Debetowej VISA Business dla umów zawartych do 30.04.2021 r., który obowiązuje pod sygnaturą CUSTOM 062022.

Informujemy również, że nowa dokumentacja będzie dostępna na stronie [www.kartybiznes.pl](http://www.kartybiznes.pl) w Strefie Administratora Programu.

W przypadku pytań prosimy o kontakt z Obsługą Kart Korporacyjnych tel: **+48 22 692 25 52** lub e-mail: [karty.obsluga.klienta@citi.com](mailto:karty.obsluga.klienta@citi.com).

**POWRÓT >>**

# Przelewy wewnętrzne: zmiany dotyczące procesowania

Miło nam poinformować, że wydłużyliśmy godziny procesowania **przelewów wewnętrznych w walucie PLN**.  
Zlecenia płatności spełniające wszystkie poniższe warunki:

- w PLN
- pomiędzy rachunkami klientów korporacyjnych w ramach Citi Handlowy
- na formacie przelewu krajowego
- złożone **do godz. 22:00**

realizowane są w tym samym dniu roboczym.

**UWAGA:** prosimy o zwrócenie szczególnej uwagi na wybór formatki zlecenia.

Inne zasady dotyczą płatności wymagających przewalutowania. Przypominamy, że zlecenia pomiędzy rachunkami w różnych walutach lub tej samej walucie obcej powinny być składane na formacie przelewu zagranicznego. Godzina graniczna przyjmowania zleceń na formacie przelewu zagranicznego lub SEPA pomiędzy rachunkami w różnych walutach lub tej samej walucie obcej (nawet, jeśli oba rachunki są w ramach Citi Handlowy) to 17:00. Zlecenia złożone po tej godzinie granicznej, na przyszłą datę waluty (dnia roboczego) powinny mieć wskazaną datę ich przeprosowania.

[POWRÓT >>](#)

# Aktualne dokumenty tożsamości: ważne ze względu na zmianę Ustawy AML

**Ze względu na wymogi wynikające ze znowelizowanej Ustawy AML przypominamy o obowiązku aktualizowania w banku dokumentów tożsamości w przypadku, gdy wygasł termin ich ważności lub nastąpiła zmiana z innych powodów. Szczegóły poniżej.**

W związku z nowelizacją Ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu z dnia 1 marca 2018 r. („Ustawa AML”), począwszy od 31 października 2021 roku, na instytucje obowiązane, w tym na banki, zostały nałożone nowe obowiązki. Są one związane ze stosowaniem środków bezpieczeństwa finansowego w sytuacji, gdy doszło do zmiany uprzednio ustalonych danych dotyczących klienta, w tym osób upoważnionych do działania w imieniu klienta lub beneficjenta rzeczywistego. Przypominamy, że cały czas banki zobowiązane są do identyfikacji klienta i weryfikacji jego tożsamości na podstawie dokumentów stwierdzających tożsamość. Citi Handlowy wykonuje te czynności w szczególności wobec osób upoważnionych do działania w imieniu klienta, czyli np. osób wskazanych w karcie wzorów podpisów lub upoważnionych do autoryzacji płatności w bankowości elektronicznej oraz posiadaczy kart korporacyjnych. Obowiązki nałożone zaktualizowaną Ustawą AML wymagają zapewnienia, że dane dotyczące klienta, w tym pochodzące z dokumentów tożsamości osób upoważnionych do działania w imieniu klienta, są aktualne. Zwracamy na to szczególną uwagę, gdyż **brak aktualnych danych może skutkować zablokowaniem możliwości wykonywania transakcji przez osobę, której dane nie są aktualne**, a to może wpłynąć na wydłużenie lub nawet wstrzymanie realizacji transakcji Państwa firmy.

[POWRÓT >>](#)

# Bankowość elektroniczna: strefa użytkownika

## Nie czekaj i wyznacz Administratora Systemu CitiDirect BE!

Administrowanie systemem CitiDirect BE jest jednym z narzędzi umożliwiających samodzielne zarządzanie rachunkiem bankowym, bez zbędnych formalności i potrzeby kontaktu z bankiem.

Administrator to funkcja nadana osobie w Państwa firmie. Administrator ma możliwość zarządzania profilami użytkowników, ich uprawnieniami oraz narzędziami autentykacyjnymi (token, MobilePASS) samodzielnie, szybko, bez konieczności kontaktu z bankiem i wysyłania dokumentacji.

W celu zapewnienia odpowiedniego wsparcia konieczne jest wskazanie co najmniej dwóch Administratorów Systemu. Bank zaleca wskazanie trzech.

### Uprawnienia Administratora Systemu:

- tworzenie i usuwanie profili użytkownika CitiDirect BE
- konfigurowanie i modyfikowanie uprawnień użytkownika
- ustawienie CitiDirect BE według własnych preferencji
- możliwość natychmiastowego zablokowania użytkownika, np. w przypadku zagubienia karty SafeWord
- generowanie raportów dotyczących uprawnień i użytkowników
- zarządzanie narzędziami autentykacyjnymi (token, MobilePASS)

Administrator Systemu może zarządzać systemem bez potrzeby wypełniania wniosków, oczekiwania na ich realizację oraz bez konieczności kontaktu z bankiem.

### Wnioski i materiały:

Nie posiadasz Administratora Systemu, by móc samodzielnie zarządzać CitiDirect BE?

[Wyznacz Administratora Systemu >>](#)

[Podręcznik dla Administratora >>](#)

Zapraszamy do kontaktu również z opiekunem CitiService.

### Korzyści wynikające z posiadania funkcji Administratora dla Firmy:

- oszczędność czasu
- bezpieczeństwo - zmiany wykonywane są dwuosobowo, po każdej zmianie wymagane są weryfikacja oraz autoryzacja
- działanie w myśl zasady „paperless”
- większa kontrola operacji dokonywanych w CitiDirect BE
- oszczędność wydatków: darmowe potwierdzenia płatności, raporty uprawnień, raporty mt940 itd.

### Jak dodawać i modyfikować uprawnienia użytkownika CitiDirect BE:

Jednym z zadań realizowanych przez Administratora Systemu CitiDirect BE jest dodawanie i modyfikacja uprawnień użytkowników. W celu ułatwienia pracy w systemie zostały stworzone szablony standardowych profili dostępu. Są to najczęściej wybierane uprawnienia (niezawierające jeszcze rachunków) zebrane w grupy.

Zapoznaj się z [instrukcją >>](#) i sprawdź, jak samodzielnie zarządzać uprawnieniami użytkowników CitiDirect BE bez zbędnych formalności i potrzeby kontaktu z bankiem.

[POWRÓT >>](#)

# Święta walut: lipiec i sierpień 2022 r.

Prezentujemy Państwu dni w **lipcu i sierpniu 2022 r.**, w których dokonane zlecenia będą realizowane następnego dnia roboczego ze względu na dni wolne od pracy w danym kraju.

LIPIEC	
1	CA, HK
4	US
3	CN, GB, HK
5	CZ, SK
6	CZ, LT
8	AE
11	AE, TR
12	TR
14	FR
15	TR
18	JP
21	BE

SIERPIEŃ	
1	AU, CA, CH, IE, IS
5	HR
9	SG, ZA
11	JP
15	Wniebowzięcie Najświętszej Maryji Panny, AT, BE, CY, ES, FR, GR, HR, IT, LT, LU, PL, PT, RO, SL
24	UA
29	GB, SK
30	TR

[POWRÓT >>](#)