komfort w biznesie

Zalecenia dotyczące bezpieczeństwa danych i środowiska pracy programu DGCS System

Spis treści

1. Cel dokumentu ... 3
2. Najważniejsza zasada – należy wykonywać kopie zapasowe ... 3
3. Kopia zapasowa a ransomware ... 4
4. Ochrona komputera i serwera ... 5
5. Ochrona przed przejęciem kont użytkowników ... 5
6. Ostrożność wobec wiadomości e-mail ... 6
7. Uprawnienia do pliku bazy danych ... 6
8. Bezpieczeństwo sieci ... 7
9. Testowanie kopii zapasowych ... 7
10. Przechowywanie danych poza siedzibą firmy ... 8
11. Minimalne zalecenia dla użytkownika programu ... 8
12. Odpowiedzialność za bezpieczeństwo środowiska ... 8
13. Podsumowanie ... 9

1. Cel dokumentu

Bezpieczeństwo danych przechowywanych w systemie informatycznym zależy nie tylko od samego programu, ale również od sposobu zabezpieczenia komputerów, serwera, sieci oraz kont użytkowników.

Program DGCS System wykorzystuje bazę danych Firebird 3.0.x i może pracować bezpośrednio na komputerze użytkownika (jednostanowiskowa baza danych) lub w architekturze klient–serwer. Program może być instalowany na komputerach z systemami: Windows, Linux oraz macOS.

Celem niniejszego dokumentu jest przedstawienie podstawowych zasad, których przestrzeganie pozwala ograniczyć ryzyko:

- utraty danych,
- kradzieży lub nieuprawnionego dostępu do danych,
- przejęcia kont użytkowników,
- zainfekowania komputera złośliwym oprogramowaniem,
- zaszyfrowania danych przez ransomware,
- przypadkowego usunięcia lub uszkodzenia bazy danych,
- utraty danych w wyniku awarii sprzętu.

UWAGA!

Żadne rozwiązanie informatyczne nie zapewnia całkowitego wyeliminowania ryzyka.

Celem stosowania opisanych poniżej zasad jest jego znaczące ograniczenie oraz zapewnienie możliwości odtworzenia danych w przypadku awarii lub incydentu bezpieczeństwa.

2. Najważniejsza zasada – należy wykonywać kopie zapasowe

Najczęstszym błędem w zakresie ochrony danych jest przekonanie, że skoro dane znajdują się na komputerze lub serwerze, to są w pełni bezpieczne. Awaria dysku, kradzież komputera, pożar, błąd użytkownika lub atak ransomware może spowodować utratę danych w ciągu kilku minut. Dlatego regularna kopia zapasowa jest najważniejszym elementem ochrony danych.

Program DGCS System wykonuje kopie bezpieczeństwa przy aktualizacji programu, ale ponadto:

- użytkownik może wykonać kopię bezpieczeństwa w dowolnym momencie,
- użytkownik może zaznaczyć, aby program wykonywał kopię bezpieczeństwa przy zamykaniu programu lub zmianie bazy danych (w przypadku pracy na wielu bazach (biura rachunkowe)).
- możliwe jest skorzystanie z modułu dodatkowego DGCS System Bezpieczne dane, który pozwala na ustawienie automatycznego harmonogramu tworzenia kopii bezpieczeństwa.

Rekomendowana Zasada 3-2-1:

- **3 kopie danych –** co najmniej 3 kopie danych (dane podstawowe oraz co najmniej 2 kopie zapasowe),
- **2 różne nośniki lub lokalizacje –** przechowywanie kopii na co najmniej 2 różnych nośnikach lub w odrębnych lokalizacjach,
- **1 kopia zewnętrzna –**przechowywana poza komputerem lub serwerem, na którym znajdują się dane produkcyjne.

  Kopie zapasowe powinny być:

  - wykonywane regularnie,
  - przechowywane w sposób uniemożliwiający ich przypadkowe usunięcie lub zaszyfrowanie,
  - zabezpieczone przed dostępem osób nieuprawnionych,
  - okresowo testowane poprzez odtworzenie danych na oddzielnej instancji testowej programu, w celu potwierdzenia możliwości ich prawidłowego odtworzenia.

Samo wykonywanie kopii nie oznacza jeszcze, że backup działa prawidłowo. Należy okresowo przeprowadzić próbne odtworzenie danych i sprawdzić, czy wykonywana kopia jest rzeczywiście możliwa do wykorzystania.

3. Kopia zapasowa a ransomware

Szczególnej uwagi wymaga ochrona przed ransomware – złośliwym oprogramowaniem, które może szyfrować pliki znajdujące się na komputerze oraz w dostępnych zasobach sieciowych. Jeżeli komputer użytkownika ma stały dostęp do folderu, w którym przechowywane są kopie zapasowe, złośliwe oprogramowanie może również uzyskać dostęp do tych kopii.

Nie zalecamy przechowywania jedynej kopii zapasowej na dysku stale podłączonym do komputera lub serwera.

Kopia zapasowa powinna być zabezpieczona w taki sposób, aby ewentualna infekcja komputera produkcyjnego nie mogła automatycznie doprowadzić do jej usunięcia lub zaszyfrowania.

Podstawą ochrony przed ransomware są:

- aktualny system operacyjny i oprogramowanie zabezpieczające,
- ograniczenie uprawnień użytkowników oraz dostępu do serwerów,
- zachowanie ostrożności przy otwieraniu załączników i linków,
- regularne kopie zapasowe przechowywane w sposób odporny na zaszyfrowanie lub usunięcie przez zainfekowany komputer.

PROCEDURA POSTĘPOWANIA W PRZYPADKU PODEJRZENIA INFEKCJI

Jeśli podejrzewasz, że Twój komputer został zainfekowany oprogramowaniem ransomware, postępuj zgodnie z poniższymi krokami:

1. Natychmiast odłącz zainfekowany komputer od sieci (wyłącz Wi-Fi, wypnij kabel Ethernet).
2. Nie kontynuuj pracy na tym komputerze i nie uruchamiaj podejrzanych plików.
3. Nie podłączaj do komputera zewnętrznych nośników z kopiami zapasowymi.
4. Niezwłocznie poinformuj dział IT lub profesjonalną firmę informatyczną.
5. Przywracanie danych z kopii zapasowej wykonuj wyłącznie po pełnym oczyszczeniu i zabezpieczeniu środowiska.

4. Ochrona komputera i serwera

Komputer, na którym pracuje program, oraz serwer przechowujący bazę danych powinny być odpowiednio zabezpieczone (dotyczy systemów Windows, Linux oraz macOS).

Zalecamy:

- regularne instalowanie aktualizacji systemu operacyjnego,
- korzystanie z aktualnego oprogramowania antywirusowego lub mechanizmów ochrony dostępnych w systemie,
- stosowanie aktywnej zapory sieciowej (firewall),
- instalowanie oprogramowania wyłącznie z zaufanych źródeł,
- ograniczenie liczby użytkowników posiadających uprawnienia administratora,
- zabezpieczenie komputerów przenośnych przed kradzieżą.

Nie należy wykorzystywać komputera przeznaczonego do przechowywania bazy danych jako stanowiska do instalowania przypadkowego oprogramowania, gier lub aplikacji pochodzących z nieznanych źródeł.

5. Ochrona przed przejęciem kont użytkowników

Przejęcie konta użytkownika może umożliwić osobie nieuprawnionej dostęp do danych, poczty elektronicznej oraz innych systemów firmy.

Zalecamy:

- stosowanie długich i unikalnych haseł oraz nieużywanie tego samego hasła w wielu systemach,
- bezwzględne nieudostępnianie haseł innym osobom,
- korzystanie z menedżerów haseł,
- stosowanie uwierzytelniania wieloskładnikowego (MFA), wszędzie tam, gdzie jest ono dostępne,
- regularne sprawdzanie listy użytkowników posiadających dostęp do systemów,
- natychmiastowe blokowanie dostępu byłym pracownikom.

WAŻNE: Zasada izolacji haseł

Hasło do jednego systemu nie powinno być wykorzystywane jako hasło do poczty e-mail, bankowości, panelu administracyjnego, serwera ani innych programów używanych w firmie.

Przejęcie jednego hasła nie powinno umożliwiać atakującemu uzyskania dostępu do wszystkich pozostałych systemów.

6. Ostrożność wobec wiadomości e-mail

Jednym z najczęstszych sposobów uzyskania dostępu do komputera jest przesłanie użytkownikowi wiadomości zawierającej złośliwy załącznik lub link.

Szczególną ostrożność należy zachować w przypadku wiadomości:

- informujących o niezapłaconej fakturze,
- zawierających rzekome dokumenty księgowe,
- informujących o przesyłce kurierskiej,
- wymagających pilnego zalogowania się,
- informujących o blokadzie konta,
- zawierających link do “potwierdzenia danych”.

Sam fakt, że wiadomość wygląda profesjonalnie i zawiera logo znanej firmy, nie oznacza, że jest autentyczna.

Przed kliknięciem linku należy sprawdzić:

- kto jest nadawcą,
- jaki jest rzeczywisty adres strony, na którą prowadzi link,
- czy wiadomość jest zgodna z wcześniejszą korespondencją,
- czy oczekiwaliśmy takiej wiadomości.

W przypadku wątpliwości bezpieczniej jest skontaktować się z nadawcą innym kanałem komunikacji.

7. Uprawnienia do pliku bazy danych

Sam dostęp do programu nie powinien być jedynym zabezpieczeniem bazy danych.

Należy również odpowiednio zabezpieczyć komputer lub serwer, na którym znajduje się plik bazy danych.

Uprawnienia systemu operacyjnego powinny być skonfigurowane w taki sposób, aby:

- dostęp do katalogu zawierającego bazę miały wyłącznie osoby i usługi, które tego wymagają,
- zwykły użytkownik nie mógł przypadkowo usunąć pliku bazy,

- osoby nieuprawnione nie miały możliwości kopiowania bazy danych,
- konto administratora systemu było odpowiednio zabezpieczone.

Konfigurację uprawnień na serwerze powinien wykonywać administrator posiadający odpowiednią wiedzę dotyczącą danego systemu operacyjnego.

8. Bezpieczeństwo sieci

Sieć komputerowa firmy powinna być zabezpieczona przed dostępem osób nieuprawnionych.

Zalecamy:

- stosowanie zapory sieciowej (firewall),
- zmianę domyślnych haseł routerów i urządzeń sieciowych,
- regularne aktualizowanie oprogramowania urządzeń sieciowych,
- stosowanie silnych haseł do sieci Wi-Fi,
- oddzielenie sieci firmowej od sieci gości,
- ograniczenie dostępu z Internetu do urządzeń znajdujących się w sieci firmowej,
- stosowanie VPN do bezpiecznego dostępu zdalnego.

Szczególną uwagę należy zwrócić na routery, serwery oraz inne urządzenia, które mogą być dostępne z Internetu.

9. Testowanie kopii zapasowych

Kopia zapasowa, której nie da się odtworzyć, nie jest skutecznym zabezpieczeniem.
Dlatego należy okresowo przeprowadzić test odtworzenia danych.

Test powinien obejmować w szczególności:

- przygotowanie środowiska testowego,
- odtworzenie kopii,
- uruchomienie programu z odtworzonej bazy danych,
- sprawdzenie podstawowych danych.

Testy powinny być wykonywane również po zmianach infrastruktury lub sposobu wykonywania kopii zapasowych.

10. Przechowywanie danych poza siedzibą firmy

Jeżeli dane są przechowywane lub kopiowane do usług zewnętrznych, należy zwrócić uwagę na:

- sposób zabezpieczenia konta,
- uwierzytelnianie wieloskładnikowe,
- szyfrowanie danych,
- lokalizację przechowywania danych,
- możliwość odzyskania danych,
- możliwości usunięcia danych,
- zakres uprawnień przyznanych dostawcy usługi.

Nie należy zakładać, że samo korzystanie z popularnej usługi internetowej oznacza automatyczne zapewnienie bezpieczeństwa danych.

11. Minimalne zalecenia dla użytkownika programu

Jeżeli klient nie posiada własnego działu IT, rekomendujemy jako absolutne minimum:

- aktualny system operacyjny,
- aktualne oprogramowanie zabezpieczające,
- silne, unikalne hasła,
- uwierzytelnienie wieloskładnikowe wszędzie tam, gdzie jest dostępne,
- ograniczenie uprawnień administratora,
- regularne kopie zapasowe bazy danych,
- co najmniej jedną kopię przechowywaną poza komputerem/serwerem produkcyjnym,
- okresowe testowanie możliwości odtworzenia kopii,
- aktualizowanie systemu i urządzeń sieciowych,
- ostrożność przy otwieraniu wiadomości e-mail i załączników.

12. Odpowiedzialność za bezpieczeństwo środowiska

DGCS S.A. ponosi odpowiedzialność za bezpieczeństwo i prawidłowe działanie oprogramowania wyłącznie w granicach jego oficjalnej specyfikacji technicznej oraz pod warunkiem stosowania przez Klienta aktualnej, wspieranej wersji systemu, spełnienia wymagań środowiskowych i regularnego wykonywania kopii zapasowych. DGCS S.A. nie ponosi odpowiedzialności za nieprawidłowe działanie systemu wynikające z awarii infrastruktury Klienta, nieuprawnionych ingerencji osób trzecich, błędów konfiguracji oraz stosowania niewspieranych wersji oprogramowania.

Bezpieczeństwo całego środowiska, w którym program jest użytkowany, zależy również od:

- systemu operacyjnego,

- konfiguracji serwera,
- konfiguracji sieci,
- zabezpieczeń urządzeń,
- uprawnień użytkowników,
- ochrony antywirusowej,
- sposobu wykonywania kopii zapasowych,
- sposobu przechowywania kopii,
- zabezpieczenia dostępu fizycznego do urządzeń.

Za prawidłową konfigurację i utrzymanie tych elementów odpowiada użytkownik lub wyznaczany przez niego administrator IT.

W przypadku braku własnego administratora IT zalecamy skorzystanie z usług profesjonalnej firmy informatycznej, która może ocenić bezpieczeństwo całej infrastruktury.

13. Podsumowanie

Bezpieczeństwo danych nie jest pojedynczym programem ani jednym ustawieniem.
Skuteczna ochrona wymaga zastosowania kilku niezależnych zabezpieczeń:

bezpieczny komputer + bezpieczna sieć + ograniczone uprawnienia + aktualne oprogramowanie + bezpieczna baza danych + regularne kopie zapasowe.

Nawet jeśli jedno z zabezpieczeń zawiedzie, pozostałe powinny ograniczyć skutki incydentu i umożliwić odzyskanie danych.

Najważniejszym elementem ochrony pozostaje regularna i sprawdzona kopia zapasowa przechowywana w sposób zabezpieczający ją przed utratą lub zaszyfrowaniem wraz z danymi produkcyjnymi.