Polityka Bezpieczeństwa firmy BC Software

Wstęp

Niniejsza Polityka Bezpieczeństwa określa zasady i procedury dotyczące ochrony danych, informacji oraz systemów informatycznych. Celem Polityki Bezpieczeństwa jest zapobieganie wszelkim zagrożeniom bezpieczeństwa, takim jak wyciek lub utrata danych, a także zapewnienie poufności, integralności i dostępności informacji.

Zakres

Polityka Bezpieczeństwa dotyczy Zarządu oraz wszystkich pracowników firmy BC Software oraz partnerów, którzy mają dostęp do poufnych informacji firmy BC Software. Niniejszym dokumentem objęte są wszystkie dane poufne przetwarzane przez firmę BC Software tj. dane , które nie zostały upublicznione (w tym dane innych organizacji przekazane do przetwarzania).

Zasady i procedury

1. **Poufność informacji**
   Informacje poufne powinny być dostępne wyłącznie dla osób uprawnionych, posiadających odpowiednie prawa dostępu. Powinna być stosowana zasada minimalnych uprawnień tj. każdy osoba/organizacji powinna posiadać tylko te uprawnienia, które są niezbędna do realizacji celów.
   - Przekazanie dostępu - opis procedury
     Przekazanie dostępu do konkretnej puli danych konkretnej osobie lub organizacji powinno mieć oficjalny charakter i powinno zostać zarejestrowane i utrwalone w formie rejestru/dokumentacji zawierającej: dane osoby przekazującej uprawnienie oraz osoby/organizacji otrzymującej uprawnienie, datę i godzinę, zakres uprawnień, zakres danych, przeznaczenie danych i cel ich przetwarzania, termin ważności dostępu. Procedura powinna obejmować autoryzację przekazania dostępu przez uprawnioną osobę lub organ odpowiedzialny za zarządzanie bezpieczeństwem informacji. Przekazanie dostępu powinno być zabezpieczone prawnie poprzez odpowiednie umowy, zgody lub decyzje autoryzacyjne, które będą narzucały obowiązek zachowania poufności przez osobę/organizację otrzymującą dostęp. Osoby otrzymujące dostęp powinny być odpowiednio przeszkolone z obowiązujących zasad bezpieczeństwa. Po oficjalnym przekazaniu dostępu należy monitorować udzielone uprawnienia w celu weryfikacji zgodności z polityką bezpieczeństwa (minimum raz na rok).
   - Odebranie dostępu - opis procedury
     Jeśli zajdzie potrzeba odebrania dostępu do danych przed upłynięciem terminu ważności dostępu - należy niezwłocznie i skutecznie odebrać dostęp jednocześnie rejestrując to zdarzenie w formie dokumentacji.

2. **Integralność**

   Informacje powinny być przetwarzane w sposób zgodny z ich przeznaczeniem i celami biznesowymi. W razie wykrycia sytuacji, w której osoba lub organizacja przetwarza dane niezgodnie z ich przeznaczeniem lub celem, który został określony na etapie przekazania - dostęp powinien zostać niezwłocznie odebrany.

3. **Dostępność**

   Informacje powinny być dostępne dla osób uprawnionych w sposób ciągły i nieprzerwany. Należy podjąć kroki ograniczające ryzyko zaburzenia ciągłości dostępu. Kroki, które należy podjąć:

   - Zapewnienie stabilności działania systemów za pośrednictwem których osoba (lub organizacja) uzyskuje dostęp do danych;
   - Wykonywanie regularnych kopii zapasowych danych (minimum raz na miesiąc, w przypadku krytycznych danych: raz na tydzień), aby nawet w razie uszkodzenia danych mieć możliwość ich szybkiego przywrócenia (zachowując ciągłość dostępu)

4. **Zarządzanie ryzykiem**

   Ryzyka związane z przetwarzaniem informacji powinny być identyfikowane i oceniane regularnie. Ryzyka uszkodzenia, wycieku lub upublicznienia danych określone na moment konstruowania niniejszego dokumentu to:

   A. *Włamanie do wewnętrznych systemów firmy i kradzież poufnych danych*
   B. *Włamanie do wewnętrznych systemów i uszkodzenie danych*
   C. *Włamanie do wewnętrznych systemów firmy i upublicznienie danych*
   D. *Uszkodzenie danych z powodu Siły Wyższej tj. pożar, huragan, wojna*
   E. *Uszkodzenie danych z powodu awarii sprzętu (serwer, komputer)*
   F. *Uszkodzenie danych przez pracownika firmy (umyślne lub niezamierzone)*
   G. *Udostępnienie poufnych danych przez pracownika firmy (umyślne lub niezamierzone)*
   H. *Wyciek danych za pośrednictwem wydrukowanych dokumentów, które nie zostały zniszczone (zabezpieczone) przed ich wyrzuceniem*
   I. *Uzyskanie dostępu do poufnych danych przez osobę nieuprawnioną poprzez "niewylogowane" urządzenie należące do uprawnionej osoby*
   J. *Uzyskanie hasła przez nieuprawnioną osobę na skutek niepożądanego utrwalenia hasła na niezabezpieczonym nośniku tj. notatnik, prywatny telefon*
   K. *Udostępnienie hasła przez pracownika na skutek oszustwa i manipulacji osób nieuprawnionych podszywających się pod inne osoby (m.in. phishing)*
   L. *Kradzież fizycznych dokumentów z biura firmy przez osoby nieupoważnione*
   M. *Kradzież komputerów/serwerów/nośników danych z biura firmy przez osoby nieupoważnione*

5. **Szkolenia pracowników**

   Pracownicy powinni być regularnie szkoleni w zakresie bezpieczeństwa informacji. Ilość i intensywność szkoleń powinna być dostosowana do poziomu odpowiedzialności i ilości uprawnień pracownika. Każdy pracownik powinien odbyć minimum jedno podstawowe szkolenie z zakresu procedur bezpieczeństwa jeszcze przed uzyskaniem dostępu do jakichkolwiek danych

Praktyki i procedury

1. Regularna zmiana haseł: Należy regularnie zmieniać hasła do systemów i aplikacji w celu zwiększenia bezpieczeństwa. Hasła powinny być zmieniane minimum raz na pół roku.
2. Stosowanie silnych haseł: Należy używać silnych haseł, które zawierają kombinację dużych i małych liter, cyfr oraz symboli. Unikaj łatwych do odgadnięcia haseł, takich jak proste ciągi znaków, daty urodzenia, czy nazwy użytkownika. Hasła powinny składać się z co najmniej 12 znaków. W przypadku krytycznych dostępów zalecane jest stosowanie haseł składających się z 18 znaków.
3. Unikalność haseł: Należy używać różnych haseł do różnych kont i usług.
4. Należy stosować Menedżera Haseł o nazwie “KeePass” do generowania i przechowywania haseł
5. Nie przechowywać haseł w niezaszyfrowanych plikach na komputerze, telefonie czy w chmurze. Nie przechowywać haseł w jawnej formie na fizycznych nośnikach np. w notatniku.
6. Nie przesyłać haseł przez niezabezpieczone kanały komunikacji, takie jak e-mail czy SMS (wyjątkiem są hasła do testowych, publicznych kont)
7. W przypadku wycieku danych lub podejrzenia naruszenia bezpieczeństwa, należy zmienić hasła do dotkniętych kont.
8. Należy zmienić hasło, jeśli zostało ono udostępnione komuś innemu, nawet jeśli było to tymczasowe.
9. Weryfikacja dwuetapowa (2FA): Gdzie to możliwe, należy stosować dwuetapową weryfikację dla dodatkowej warstwy bezpieczeństwa.
10. Dokumenty przeznaczone do utylizacji zawierające poufne dane powinny być w pierwszej kolejności zniszczone w niszczarce.
11. Cyfrowe nośniki danych przeznaczone do utylizacji powinny być najpierw sformatowane, a następnie fizycznie zniszczone w takim sposób aby uniemożliwić odzyskanie danych
12. Aktualizacje systemów: Regularne aktualizacje krytycznych systemów operacyjnych i aplikacji w celu zapobiegania lukom w zabezpieczeniach. Dotyczy to również aktualizacji systemów operacyjnych oraz bibliotek używanych w rozwijanych aplikacjach.
13. Zarządzanie uprawnieniami: Precyzyjne zarządzanie uprawnieniami dostępu do danych i zasobów systemowych.
14. Szkolenia z bezpieczeństwa: Regularne szkolenia pracowników z zakresu bezpieczeństwa IT i świadomości zagrożeń.
15. Szyfrowanie danych: Wdrożenie szyfrowania danych przechowywanych i przesyłanych w firmie, przede wszystkich tych danych, które z różnych względów muszą być przesyłane za pośrednictwem globalnej sieci.
16. Ochrona przed atakami: Wdrożenie rozwiązań technicznych zabezpieczających przed atakami typu phishing, malware, ransomware itp.
17. Dane, które nie są i nie będą przetwarzane powinny zostać usunięte. Szczególnie w przypadku, gdy mówimy o Danych Osobowych.
18. Na prośbę właściciela, Dane Osobowe powinny zostać natychmiast usunięte zgodnie z obowiązującymi przepisami dotyczącymi Danych Osobowych RODO
19. Ochrona przed złośliwym oprogramowaniem: Każde urządzenie przetwarzające dane firmy powinny być wyposażone w najnowsze oprogramowanie antywirusowe

20. Tworzenie i odtwarzanie kopii zapasowych: Regularne tworzenie i testowanie kopii zapasowych danych w celu zapewnienia spójności i dostępności w przypadku awarii.

    Procedura tworzenia kopii zapasowej (minimum raz na 2-tygodnie):

    - Uruchomienie skryptu generującego kopie zapasową dla ba danych / plików
    - Zabezpieczenie plików z kopią zapasową na minimum dwóch niezależnych od siebie nośnikach (tak aby ewentualna awaria jednego z nich nie miała wpływu na drugi). Rekomendowane nośniki to: nośnik offline (niewymagający podłączenia do globalnej sieci w celu uzyskania dostępu) np. dysk twardy w komputerze lub dysk zewnętrzny oraz nośnik online, najlepiej "chmura" zaufanego dostawcy, który gwarantuje dodatkowe zabezpieczenia
    - Wykonanie testu odtworzenia danych z kopii w celu upewnienia się, że kopia nie jest uszkodzona i gwarantuje odtworzenie danych w razie awarii

    Procedura odtwarzania kopii zapasowej:

    - W razie wystąpienia awarii należy w pierwszej kolejności zabezpieczyć produkcyjne dane (bazy danych, pliki) nawet jeśli są uszkodzone (w celu ich ewentualnej naprawy lub przywrócenia)
    - Zidentyfikować zakres uszkodzonych danych
    - Odnaleźć i przygotować najbardziej aktualną kopię zapasową
    - Przywrócić kopię zapasową odpowiednim skryptem nadpisując uszkodzone dane
    - Wykonać testy danych/systemów po przywróceniu danych z kopii
    - Udostępnić klientom/użytkownikom działający system/dane
    - Przeprowadzić analizę opłacalności naprawy uszkodzonych danych (uszkodzone dane mogą zawierać cenne informacje, które akurat nie zostały jeszcze wytworzone w momencie tworzenia najnowszej kopii zapasowej)

    Minimalny interwał to raz na 2-tygodnie. Zalecany interwał wykonywania kopii (szczególnie w przypadku systemów real-time) to raz na dobę (w godzinach nocnych).

21. Audyt bezpieczeństwa: Regularne przeprowadzanie audytów bezpieczeństwa wewnętrznych i zewnętrznych w celu oceny i poprawy stanu zabezpieczeń.

Zarządzanie incydentami bezpieczeństwa

Możliwe rodzaje incydentów i konkretne kroki, które należy wykonać w reakcji na każdy z nich:

1. Utrata Danych Osobowych:

Identyfikacja i ocena incydentu: Szybko zidentyfikować, co zostało utracone, jak doszło do utraty, i które dane są dotknięte.

Zawiadomienie odpowiednich organów: Jeśli incydent może spowodować ryzyko dla praw i wolności osób fizycznych, należy powiadomić odpowiedni organ nadzorczy w ciągu 72 godzin.

Komunikacja z osobami dotkniętymi: Jeśli incydent stwarza wysokie ryzyko dla praw i wolności osób, należy niezwłocznie powiadomić osoby, których dane dotyczą.

Środki zaradcze: Podjąć działania, aby ograniczyć skutki utraty danych i zapobiec powtórzeniu się incydentu.

2. Nieautoryzowany dostęp do danych osobowych:

Identyfikacja incydentu: Szybko ustalić zakres naruszenia, rodzaje dostępnych danych i liczbę osób dotkniętych.

Zawiadomienie organu nadzorczego i osób dotkniętych: Postępować zgodnie z procedurami zawiadomień, jak w przypadku utraty danych.

Analiza przyczyn i środki zaradcze: Zidentyfikować, jak doszło do naruszenia, i wdrożyć środki mające na celu zapobieganie przyszłym incydentom.

3. Naruszenie integralności danych (np. zmiana danych bez autoryzacji):

Ocena skutków: Ustalić, jakie dane zostały zmienione i jakie mogą być tego konsekwencje.

Przywrócenie danych: O ile to możliwe, przywrócić dane do ich pierwotnego stanu.

Zawiadomienie odpowiednich stron: W razie potrzeby poinformować organy nadzorcze i osoby dotknięte.

4. Naruszenie dostępności danych (np. atak ransomware):

Szybka reakcja: Podjąć kroki w celu przywrócenia dostępu do danych, np. przez przywrócenie z kopii zapasowych.

Analiza i środki zaradcze: Zrozumieć przyczynę ataku i wdrożyć środki zapobiegające podobnym incydentom w przyszłości.

5. Wyciek danych przez pracowników:

Śledztwo wewnętrzne: Zbadać, jak doszło do wycieku i kto jest za niego odpowiedzialny.

Działania dyscyplinarne: Podjąć odpowiednie kroki wobec osoby/osób odpowiedzialnych.

Informowanie odpowiednich stron: Zawiadomić organy nadzorcze i osoby dotknięte, jeśli jest to wymagane.

W każdym przypadku, oprócz powyższych kroków, ważne jest również:

Dokumentacja incydentu: Zapisywać wszystkie działania podjęte w odpowiedzi na incydent, w tym szczegóły samego incydentu, podjęte działania i ich efekty.

Przegląd i aktualizacja polityk bezpieczeństwa: Regularnie przeglądać i aktualizować polityki i procedury bezpieczeństwa, aby lepiej zapobiegać przyszłym incydentom.

Przeprowadzanie audytów i testów penetracyjnych: Regularne audyty i testy penetracyjne mogą pomóc w identyfikacji potencjalnych luk w zabezpieczeniach i zapobiegać naruszeniom bezpieczeństwa.

Współpraca z ekspertami zewnętrznymi: W przypadkach skomplikowanych incydentów, rozważenie współpracy z ekspertami zewnętrznymi w zakresie bezpieczeństwa cyfrowego i ochrony danych osobowych.

Analiza post-incydentowa: Po rozwiązaniu incydentu przeprowadzić szczegółową analizę, aby zrozumieć jego przyczyny i zidentyfikować obszary wymagające poprawy.

Komunikacja wewnętrzna i zewnętrzna: Zapewnić, że wszyscy pracownicy są świadomi procedur dotyczących incydentów bezpieczeństwa, a także utrzymywać otwartą komunikację z klientami i partnerami biznesowymi w zakresie ochrony danych.

Wdrożenie Polityki Bezpieczeństwa

Polityka Bezpieczeństwa jest obowiązująca dla wszystkich pracowników, kontrahentów i partnerów biznesowych, którzy przetwarzają wewnętrzne dane firmy BC Software. Wdrożenie Polityki Bezpieczeństwa jest zadaniem Zarządu, który jest odpowiedzialny za zapewnienie, że wszyscy pracownicy są świadomi zasad i procedur dotyczących bezpieczeństwa informacji.

Aktualizacje Polityki Bezpieczeństwa

Polityka Bezpieczeństwa jest regularnie monitorowana i audytowana, aby zapewnić, że jest skuteczna w minimalizowaniu ryzyka związanego z przetwarzaniem informacji. Taki audyt Polityki Bezpieczeństwa powinien być przeprowadzany minimum raz na rok.