Poniższe informacje dotyczące bezpieczeństwa zostały przygotowane na gruncie wymagań Rozporządzenia (UE) 2023/988 w sprawie ogólnego bezpieczeństwa produktów (zwanego GPSR). Ich celem jest zapewnienie jak najleszej ochrony użytkowników przed potencjalnymi zagrożeniami wynikającymi z nieodpowiedniego użytkowania produktów. Wszystkie informacje dotyczące bezpieczeństwa zostały sformułowane w prosty i zrozumiały sposób, tak aby były dostępne dla wszystkich użytkowników.

Instrukcja bezpieczeństwa dla Programów Serwerowych

1. **Aktualizacje i Patches**
   - Regularnie aktualizuj oprogramowanie serwerowe do najnowszych wersji. Zapewnia to dostęp do zabezpieczeń i poprawek błędów.
   - Konfiguruj automatyczne powiadomienia o dostępnych aktualizacjach.

2. **Zarządzanie dostępem**
   - Ustal zasady dotyczące silnych haseł. Użytkownicy powinni stosować hasła skomplikowane, zmieniać je regularnie i nie udostępniać innym.
   - Wdróż system ról, aby ograniczyć dostęp do wrażliwych danych i funkcji serwera.

3. **Zabezpieczenia sieciowe**
   - Skonfiguruj zaporę ogniową (firewall) w celu ochrony serwera przed nieautoryzowanym dostępem.
   - Używaj sieci VPN do zdalnego dostępu do serwera w celu zabezpieczenia przesyłanych danych.

4. **Monitorowanie i Audyty**
   - Regularnie monitoruj dzienniki aktywności (logs) w celu wykrywania nieprawidłowości i potencjalnych zagrożeń.
   - Przeprowadzaj audyty bezpieczeństwa co najmniej raz na rok, aby zidentyfikować słabe punkty w infrastrukturze.

5. **Kopie zapasowe**
   - Regularnie wykonuj kopie zapasowe danych i konfiguracji serwera. Przechowuj kopie w bezpiecznej lokalizacji.
   - Sprawdzaj integralność kopii zapasowych, aby upewnić się, że można je przywrócić w razie potrzeby.

6. **Ochrona przed złośliwym oprogramowaniem**
   - Zainstaluj oprogramowanie antywirusowe i zapewnij jego regularne aktualizacje.
   - Regularnie skanować serwer w poszukiwaniu potencjalnych zagrożeń.

7. **Bezpieczne protokoły komunikacji**
   - Używaj szyfrowanych protokołów (np. HTTPS, SFTP) do przesyłania danych.
   - Unikaj korzystania z przestarzałych protokołów, które mogą nie zapewniać odpowiedniego poziomu bezpieczeństwa.

8. **Przeszkolenie personelu**
   - Regularnie organizuj szkolenia dla pracowników na temat najlepszych praktyk w zakresie bezpieczeństwa IT.
   - Zwiększaj świadomość na temat zagrożeń, takich jak phishing czy inżynieria społeczna.

9. **Plan reakcji na incydenty**
   - Sporządź i przetestuj plan reakcji na incydenty w przypadku naruszenia bezpieczeństwa.

- Zidentyfikuj kluczowe osoby odpowiedzialne za zarządzanie bezpieczeństwem oraz ich role w przypadku incydentów.

10. **Dokumentacja**
    - Prowadź szczegółową dokumentację wszystkich procesów i procedur związanych z bezpieczeństwem serwera.
    - Wszelkie zmiany w konfiguracji lub politykach bezpieczeństwa powinny być odpowiednio udokumentowane.

Przestrzeganie powyższych zasad pozwoli zminimalizować ryzyko związane z bezpieczeństwem programów serwerowych.

Dodatkowe szczegółowe ostrzeżenia oraz informacje dotyczące bezpieczeństwa produktu i jego użytkowania są dostępne w instrukcji obsługi dołączonej do produktu, instrukcji w formacie pdf, w karcie produktu lub na stronie internetowej producenta i/albo dystrybutora.