

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 najlepszej 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 Przełączników KVM

1. Wprowadzenie

Przełączniki KVM (Keyboard, Video, Mouse) są urządzeniami umożliwiającymi kontrolowanie wielu komputerów z jednego zestawu klawiatury, monitora i myszy. Ze względu na ich kluczową rolę w infrastrukturze IT, istotne jest przestrzeganie zasad bezpieczeństwa, aby chronić dane oraz urządzenia.

2. Wymagania wstępne

- Upewnij się, że przełącznik KVM jest zgodny z aktualnymi standardami i normami bezpieczeństwa.
- Przeprowadzaj regularne audyty sprzętu i oprogramowania.

3. Fizyczne bezpieczeństwo

- Umieść przełącznik KVM w zamkniętym pomieszczeniu, dostępnym tylko dla uprawnionych użytkowników.
- Zabezpiecz przewody i złącza, aby zminimalizować ryzyko przypadkowego odłączenia lub uszkodzenia.
- Regularnie sprawdzaj stan urządzenia, monitorując oznaki nieautoryzowanego dostępu.

4. Bezpieczeństwo oprogramowania

- Zmieniaj domyślne hasła do zarządzania przełącznikiem KVM na silne, unikalne hasła.
- Regularnie aktualizuj oprogramowanie przełącznika KVM do najnowszych wersji, aby eliminować znane luki bezpieczeństwa.
- Używaj oprogramowania zabezpieczającego do monitorowania aktywności na urządzeniu.

5. Zasady użytkowania

- Edukuj użytkowników o znaczeniu zachowania poufności haseł i dostępu do urządzeń.
- Wprowadź procedury logowania i wylogowywania użytkowników, aby zapobiec nieautoryzowanemu dostępowi.
- Ogranicz dostęp do przełącznika KVM tylko do wyznaczonych osób.

6. Zarządzanie dostępem

- Ustal zasady przyznawania i odbierania dostępu do systemu.
- Regularnie przeglądaj i aktualizuj listę użytkowników z dostępem do przełącznika KVM.
- Wykorzystuj techniki uwierzytelniania wieloskładnikowego, jeśli to możliwe.

7. Monitorowanie i audyt

- Prowadź logi dostępu do przełącznika oraz wszelkich zdarzeń w systemie.
- Regularnie przeglądaj logi w celu wykrywania nieautoryzowanych prób dostępu.
- Przeprowadzaj okresowe audyty bezpieczeństwa, aby zapewnić zgodność z politykami bezpieczeństwa.

8. Postępowanie w przypadku incydentów

- Opracuj plan reagowania na incydenty bezpieczeństwa związane z przełącznikami KVM.
- W przypadku wykrycia naruszenia bezpieczeństwa natychmiast powiadom odpowiednie

osoby w organizacji.

- Dokumentuj wszystkie incydenty, aby analizować ich przyczyny i wprowadzać poprawki w politykach bezpieczeństwa.

9. Szkolenia i świadomość

- Organizuj regularne szkolenia dla pracowników w zakresie bezpieczeństwa IT i korzystania z przełączników KVM.
- Promuj kulturę bezpieczeństwa w organizacji, zachęcając pracowników do zgłaszania podejrzanych działań.

Przestrzeganie powyższych zasad pomoże w minimalizacji ryzyka związane z używaniem przełączników KVM oraz ochroni systemy i dane organizacji.

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.