Instrukcja Bezpieczeństwa - Systemy Operacyjne

Zgodna z wymogami Rozporządzenia (UE) 2023/988 - GPSR

Wprowadzenie:

Niniejsza instrukcja bezpieczeństwa zawiera ważne informacje dotyczące bezpiecznego użytkowania systemów operacyjnych (dalej: "SO"). Prosimy o dokładne zapoznanie się z nią przed rozpoczęciem użytkowania SO. Należy przestrzegać wszystkich zaleceń i ostrzeżeń zawartych w niniejszym dokumencie.

Zagrożenia związane z użytkowaniem Systemów Operacyjnych:

- **Złośliwe oprogramowanie (Malware):** Wirusy, trojany, robaki, ransomware i inne rodzaje złośliwego oprogramowania mogą zainfekować SO i uszkodzić dane, zakłócić działanie systemu lub przejąć kontrolę nad urządzeniem.
- **Luki w zabezpieczeniach:** SO, podobnie jak każde oprogramowanie, mogą zawierać luki w zabezpieczeniach, które mogą zostać wykorzystane przez osoby nieuprawnione do uzyskania dostępu do systemu i danych.
- **Phishing i Socjotechnika:** Próby wyłudzenia informacji osobistych lub danych logowania poprzez podszywanie się pod zaufane podmioty.
- **Niezabezpieczone połączenia sieciowe:** Korzystanie z niezabezpieczonych sieci Wi-Fi (np. publicznych) może narazić dane na przechwycenie.
- **Utrata danych:** Awaria sprzętu, błędy oprogramowania lub działanie złośliwego oprogramowania mogą prowadzić do utraty danych.
- **Nieautoryzowany dostęp:** Osoby nieuprawnione mogą uzyskać dostęp do SO i danych, jeśli nie są zastosowane odpowiednie środki bezpieczeństwa.
- **Aktualizacje:** Brak aktualizacji SO do najnowszych wersji może prowadzić do luk w zabezpieczeniach.

Środki Ostrożności i Zalecenia dotyczące Bezpiecznego Użytkowania:

1. **Aktualizacje Systemu:**
    - Regularnie instaluj aktualizacje SO, w tym aktualizacje zabezpieczeń. Upewnij się, że funkcja automatycznych aktualizacji jest włączona.
    - Aktualizuj sterowniki sprzętu do najnowszych wersji udostępnianych przez producenta.
2. **Oprogramowanie Antywirusowe i Firewall:**

- Zainstaluj i regularnie aktualizuj oprogramowanie antywirusowe renomowanego producenta.
- Włącz i skonfiguruj firewall (zapora sieciowa) dostarczany z SO lub zainstaluj oddzielne oprogramowanie firewall.
- Regularnie skanuj system w poszukiwaniu złośliwego oprogramowania.

3. **Hasła i Uwierzytelnianie:**
   - Używaj silnych haseł (składających się z co najmniej 12 znaków, zawierających kombinację dużych i małych liter, cyfr i znaków specjalnych) do logowania się do SO i kont użytkowników.
   - Unikaj używania tego samego hasła do różnych kont.
   - W miarę możliwości włącz uwierzytelnianie dwuskładnikowe (2FA) dla kont użytkowników.
   - Regularnie zmieniaj hasła.
4. **Podejrzane Linki i Załączniki:**
   - Unikaj klikania w podejrzane linki i otwierania załączników od nieznanych nadawców.
   - Zachowaj ostrożność podczas pobierania plików z Internetu, upewnij się, że pochodzą one z zaufanych źródeł.
   - Nie ujawniaj swoich danych osobowych ani danych logowania w odpowiedzi na podejrzane e-maile lub wiadomości.
5. **Bezpieczeństwo Sieci:**
   - Korzystaj z bezpiecznych połączeń sieciowych (np. własnej sieci Wi-Fi z silnym hasłem).
   - Unikaj korzystania z publicznych, niezabezpieczonych sieci Wi-Fi. Jeśli musisz z nich korzystać, używaj sieci VPN (Virtual Private Network).
   - Wyłącz funkcję udostępniania plików i drukarek, jeśli nie jest potrzebna.
6. **Kopie Zapasowe (Backup):**
   - Regularnie twórz kopie zapasowe ważnych danych.
   - Przechowuj kopie zapasowe na oddzielnym nośniku lub w chmurze.
   - Regularnie testuj odtwarzanie danych z kopii zapasowej.

7. **Uprawnienia Użytkowników:**
    - Ogranicz uprawnienia użytkowników do niezbędnego minimum.
    - Używaj konta z uprawnieniami administratora tylko w razie potrzeby.
    - Utwórz oddzielne konto użytkownika do codziennej pracy z ograniczonymi uprawnieniami.
8. **Bezpieczne Przeglądanie Internetu:**
    - Używaj aktualnej przeglądarki internetowej z włączonymi funkcjami bezpieczeństwa.
    - Używaj wtyczek blokujących reklamy i skrypty śledzące.
    - Zachowaj ostrożność podczas odwiedzania stron internetowych o nieznanej reputacji.
    - Sprawdzaj, czy strony internetowe używają protokołu HTTPS (symbol kłódki w pasku adresu).
9. **Monitorowanie Systemu:**
    - Monitoruj działanie SO i sprawdzaj dzienniki systemowe w poszukiwaniu podejrzanych aktywności.
    - W przypadku wykrycia podejrzanej aktywności niezwłocznie odłącz urządzenie od sieci i przeskanuj system oprogramowaniem antywirusowym.
10. **Bezpieczne Utylizowanie:**
    - Przed utylizacją urządzenia zawierającego SO, bezpiecznie usuń wszystkie dane.
    - Użyj specjalnego oprogramowania do trwałego usuwania danych (np. DBAN).
    - Sformatuj dysk twardy i nadpisz dane kilkukrotnie.
11. **Ochrona Danych Osobowych:**
    - Bądź świadomy informacji, które udostępniasz online.
    - Ograniczaj udostępnianie danych osobowych na portalach społecznościowych i innych stronach internetowych.
    - Zwracaj uwagę na ustawienia prywatności w SO i aplikacjach.

Postępowanie w Przypadku Naruszenia Bezpieczeństwa:

W przypadku podejrzenia naruszenia bezpieczeństwa (np. infekcja złośliwym oprogramowaniem, nieautoryzowany dostęp) należy niezwłocznie podjąć następujące kroki:

- Odłącz urządzenie od sieci (Internet, sieć lokalna).
- Uruchom skanowanie antywirusowe w trybie awaryjnym.
- Zmień hasła do wszystkich kont użytkowników.
- Poinformuj administratora systemu (jeśli dotyczy).
- Rozważ ponowną instalację SO (jako ostateczność).

Ograniczenie Odpowiedzialności:

Niniejsza instrukcja bezpieczeństwa zawiera ogólne zalecenia dotyczące bezpiecznego użytkowania SO. Nie gwarantuje ona całkowitej ochrony przed wszystkimi zagrożeniami. Użytkownik ponosi pełną odpowiedzialność za podjęcie odpowiednich środków bezpieczeństwa i przestrzeganie zaleceń zawartych w niniejszym dokumencie.

Niniejsza instrukcja bezpieczeństwa może być aktualizowana. Zalecamy regularne sprawdzanie najnowszej wersji.