Ostrzeżenia dotyczące bezpieczeństwa dla oprogramowania antywirusowego

(Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2023/988 w sprawie ogólnego bezpieczeństwa produktów – GPSR)

Ważne! Oprogramowanie antywirusowe jest fundamentem ochrony cyfrowej, ale nie jest narzędziem nieomylnym. Niewłaściwa konfiguracja, instalacja wielu antywirusów jednocześnie lub fałszywe poczucie bezpieczeństwa mogą prowadzić do paraliżu systemu, kradzieży tożsamości oraz utraty środków finansowych.

1. Zasada jednego antywirusa (Krytyczne)

- **Konflikty systemowe (Krytyczne):** Nigdy nie instaluj dwóch różnych programów antywirusowych z aktywną ochroną w czasie rzeczywistym na jednym urządzeniu. Programy te będą traktować nawzajem swoje działania jako podejrzane, co doprowadzi do drastycznego spadku wydajności, zawieszania się systemu (tzw. "zamrożenie") lub całkowitego braku ochrony przez blokowanie wzajemnych silników skanujących.
- **Wbudowane zabezpieczenia:** Współczesne systemy (np. Windows 11) mają wbudowaną ochronę (Windows Defender). Instalacja zewnętrznego antywirusa zazwyczaj automatycznie go dezaktywuje, co jest procesem prawidłowym.

2. Bezpieczeństwo źródła i instalacji

- **Oficjalne kanały (Krytyczne):** Pobieraj instalatory wyłącznie ze stron producentów lub autoryzowanych sklepów (np. Google Play, App Store). Instalacja "darmowych wersji pro" z torrentów lub nieznanych forów to najkrótsza droga do zainfekowania komputera trojanem typu "stealer", który wykradnie hasła do bankowości, zanim antywirus w ogóle się uruchomi.
- **Klucze aktywacyjne:** Unikaj kupowania kluczy na portalach aukcyjnych od sprzedawców oferujących ceny o 90% niższe niż

rynkowe. Takie klucze często pochodzą z kradzieży kart kredytowych i mogą zostać zablokowane przez producenta w dowolnym momencie, pozostawiając Cię bez ochrony.

3. Ograniczenia ochrony (Fałszywe poczucie bezpieczeństwa)

- **Inżynieria społeczna (Krytyczne):** Antywirus nie uchroni Cię przed Tobą samym. Jeśli dobrowolnie podasz hasło na fałszywej stronie banku (phishing) lub zatwierdzisz transakcję w aplikacji mobilnej, program może nie zdążyć zareagować. Zawsze weryfikuj adres URL strony, na której podajesz wrażliwe dane.
- **Zagrożenia typu Zero-Day:** Żaden antywirus nie wykrywa 100% zagrożeń. Nowo powstałe wirusy mogą nie znajdować się jeszcze w bazach sygnatur. Dlatego kluczowe jest regularne aktualizowanie bazy definicji (zazwyczaj odbywa się to automatycznie).

4. Prywatność i zbieranie danych

- **Analiza behawioralna:** Większość nowoczesnych antywirusów przesyła anonimowe dane o podejrzanych plikach do chmury producenta w celu ich analizy. Jeśli pracujesz na skrajnie poufnych dokumentach, sprawdź w ustawieniach prywatności, jakie dane są wysyłane poza Twoje urządzenie.
- **Uprawnienia administratora:** Program antywirusowy wymaga najwyższych uprawnień systemowych (Root/Admin), aby skutecznie skanować pliki. Powierzasz mu pełną kontrolę nad swoim urządzeniem, dlatego wybieraj firmy o ugruntowanej reputacji i przejrzystej polityce prywatności.

5. Wydajność i ergonomia pracy

- **Skanowanie w tle:** Planuj pełne skanowanie systemu na godziny, w których nie korzystasz intensywnie z komputera (np. przerwa obiadowa). Pełny skan obciąża dysk i procesor, co może powodować opóźnienia w pracy aplikacji profesjonalnych lub grach.

- **Tryb gry/prezentacji:** Korzystaj z funkcji wyciszania powiadomień. Nagłe wyskakujące okno o aktualizacji bazy wirusów podczas ważnej prezentacji lub rozgrywki online może być uciążliwe.

6. Dezinstalacja i utylizacja danych

- **Całkowite usuwanie:** Zwykłe odinstalowanie antywirusa przez panel sterowania często pozostawia resztki plików, które mogą spowalniać system. Producenci zazwyczaj udostępniają dedykowane narzędzia do całkowitego usuwania oprogramowania (tzw. Removal Tools).
- **Kopia zapasowa (Backup):** Antywirus może w kwarantannie zablokować plik, który uznasz za bezpieczny (False Positive). Zawsze miej kopię zapasową swoich najważniejszych danych na zewnętrznym nośniku niepodłączonym na stałe do komputera.