**Rekomendacje dot. oprogramowania Kaspersky Q&A**

**Q: Jak działa oprogramowanie antywirusowe i jak korzystanie z niego może stanowić zagrożenie dla bezpieczeństwa?**

A: Oprogramowanie antywirusowe w celu skutecznego działania wymaga wysokich uprawnień w systemie operacyjnym. Aby wykrywać złośliwe oprogramowanie, program antywirusowy posiada na chronionym komputerze dostęp do treści plików, programów i połączeń sieciowych. Oprócz skanowania plików na komputerze, pewne informacje wysyłane są na serwery producenta oprogramowania antywirusowego. W skrajnym przypadku zachodzi ryzyko przekazania pozyskanych informacji podmiotom trzecim, w tym służbom specjalnym kraju, w którym producent ma główną siedzibę.

Oprogramowanie antywirusowe, aby być skutecznym narzędziem wykrywania i zwalczania szkodliwego oprogramowania, wymaga ciągłych uaktualnień, tak aby nadążać za nowymi rodzajami ataków. Użytkownik oprogramowania antywirusowego musi posiadać zaufanie do jego producenta, że dochował on należytej staranności i uwzględnił wszystkie znane wzorce ataków oraz, że w uaktualnieniach nie ma fragmentów kodu, który w przyszłości może być wykorzystany do przeprowadzenia ataku.

**Q: Jako podmiot krajowego systemu cyberbezpieczeństwa** **korzystam z oprogramowania antywirusowego firmy Kaspersky Lab. Czy w związku z rekomendacją mam je natychmiast usunąć?**

A: Wycofanie ze stosowania produktów firmy Kaspersky Lab powinno być poprzedzone przeprowadzeniem szacowania ryzyka, obejmującego zarówno ryzyka związane z wycofaniem, jak i z dalszym stosowaniem produktów tej firmy.

Rekomenduje się jak najszybsze przestanie korzystania z oprogramowania Kaspersky Lab. Jeżeli musisz dalej korzystać z oprogramowania Kaspersky Lab, to w panelu administracyjnym tego oprogramowania maksymalnie ogranicz wysyłanie danych na serwery zewnętrzne. Jednocześnie pamiętaj, że w oprogramowaniu tym mogą pozostawać nieudokumentowane funkcjonalności, które mogą stać się drogą do ataku na Twój system.

**Q: Mam obowiązek stosowania ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych. Czy mogę odrzucić ofertę wykonawcy, który oferuje produkty firmy Kaspersky Lab? Co z możliwością wykluczenia zamawiającego?**

A: Należy ją odrzucić, ponieważ rekomendacja stwierdza negatywny wpływ na bezpieczeństwo publiczne oprogramowania Kaspersky Lab.

W przypadku udzielania zamówień w trybie przepisów ustawy - Prawo zamówień publicznych, na podstawie art. 226 ust. 1 ustawy PZP, zamawiający odrzuca ofertę wykonawcy, jeżeli obejmuje ona urządzenia informatyczne lub oprogramowanie wskazane w rekomendacji, o której mowa w art. 33 ust. 4 ustawy o Krajowym Systemie Cyberbezpieczeństwa, stwierdzającej ich negatywny wpływ na bezpieczeństwo publiczne lub bezpieczeństwo narodowe.

W postępowaniach o udzielenie zamówienia publicznego w dziedzinach obronności i bezpieczeństwa zamawiający może wykluczyć wykonawcę, oferującego oprogramowanie Kaspersky Lab, również na podstawie art. 405 ust. 2 pkt 3, z uwagi na brak wiarygodności firmy Kaspersky Lab niezbędnej do wykluczenia zagrożenia dla obronności lub bezpieczeństwa państwa. Za wspomniany w przepisie „inny sposób”, należy w tym przypadku uznać rekomendację Pełnomocnika Rządu do spraw Cyberbezpieczeństwa.

Q: **Kogo dotyczy rekomendacja?**

A: Rekomendacja dotyczy podmiotów Krajowego Systemu Cyberbezpieczeństwa, wymienionych w art. 4 ustawy o Krajowym Systemie Cyberbezpieczeństwa, a w szczególności:

* operatorów usług kluczowych;
* dostawców usług cyfrowych;
* CSIRT MON;
* CSIRT NASK;
* CSIRT GOV;
* sektorowych zespołów cyberbezpieczeństwa;
* jednostek sektora finansów publicznych, o których mowa w art. 9 pkt 1–6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;
* instytutów badawczych;
* Narodowego Banku Polskiego;
* Banku Gospodarstwa Krajowego;
* Urzędu Dozoru Technicznego;
* Polskiej Agencji Żeglugi Powietrznej;
* Polskiego Centrum Akredytacji;
* Narodowego Funduszu Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkich funduszy ochrony środowiska i gospodarki wodnej;
* spółek prawa handlowego wykonujących zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej;
* podmiotów świadczących usługi z zakresu cyberbezpieczeństwa;
* organów właściwych do spraw cyberbezpieczeństwa.

**Q:** **Kto wchodzi w skład Kolegium do Spraw Cyberbezpieczeństwa?**

A: W skład Kolegium, zgodnie z art. 66 ustawy o Krajowym Systemie Cyberbezpieczeństwa, wchodzą:

* przewodniczący Kolegium – Prezes Rady Ministrów;
* Pełnomocnik Rządu do spraw Cyberbezpieczeństwa;
* sekretarz Kolegium;
* członkowie Kolegium:
	+ minister właściwy do spraw wewnętrznych,
	+ minister właściwy do spraw informatyzacji,
	+ Minister Obrony Narodowej,
	+ minister właściwy do spraw zagranicznych,
	+ Szef Kancelarii Prezesa Rady Ministrów,
	+ Szef Biura Bezpieczeństwa Narodowego, jeżeli został wyznaczony przez Prezydenta Rzeczypospolitej Polskiej,
	+ minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych lub osoba przez niego upoważniona w randze sekretarza stanu albo podsekretarza stanu, a jeżeli minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego.

**Q: Czy rekomendacja ma zastosowanie wobec przedsiębiorcy telekomunikacyjnego?**

A: Operator może mieć obowiązek z mocy prawa do uwzględnienia rekomendacji.

Przedsiębiorca telekomunikacyjny dostarczający sieć piątej generacji (5G), na podstawie § 3 ust. 1 pkt 1 rozporządzenia Ministra Cyfryzacji z dnia 22 czerwca 2020 r. wsprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usługuwzględnia rekomendacje, o których mowa w art. 33 ust. 4 ustawy o Krajowym Systemie Cyberbezpieczeństwa.

**Q: Czy rekomendacja ma zastosowanie wobec operatora pocztowego?**

A: Operator pocztowy może mieć obowiązek z mocy prawa do wdrożenia rekomendacji.

Operator pocztowy, który świadczy usługi na obszarze większym niż województwo lub którego roczne przychody z tytułu wykonywania działalności pocztowej w poprzednim roku obrotowym były większe od kwoty 400 tysięcy złotych, sporządzając plan działania w sytuacji szczególnego zagrożenia, na podstawie § 7 pkt 9 w zw. z § 2 rozporządzenia Rady Ministrów z dnia 23 lipca 2021 r. w sprawie planów działania operatora pocztowego w sytuacji szczególnego zagrożenia,uwzględnia w tym planie opis sposobu wdrożenia rekomendacji z art. 33 ust. 4 ustawy o Krajowym Systemie Cyberbezpieczeństwa.

**Q: W jaki sposób mogę odnieść się do rekomendacji?**

A: Podmiot Krajowego Systemu Cyberbezpieczeństwa może wnieść do Pełnomocnika Rządu do spraw Cyberbezpieczeństwa zastrzeżenia do rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania, z uwagi na ich negatywny wpływ na świadczoną usługę lub realizowane zadanie publiczne, nie później niż w terminie 7 dni od dnia otrzymania rekomendacji. Pełnomocnik odnosi się do zastrzeżeń niezwłocznie, jednak nie później niż w terminie 14 dni od dnia ich otrzymania. W efekcie Pełnomocnik podtrzyma, nie zmieni rekomendacji lub wyda je zmienione.