Wiceprezes Rady Ministrów
Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

KOMUNIKAT

w sprawie zagrożeń związanych z wyborami prezydenckimi

W trakcie wyborów, które odbywały się w Polsce w ubiegłych latach, obserwowane były nasilone działania w cyberprzestrzeni ze strony nieprzyjaznych państw. Próby ingerencji w procesy wyborcze za pomocą działań w sferze cyfrowej obserwowane są także w innych państwach. Polska mierzy się z cyberatakami i innymi działaniami hybrydowymi powiązanymi z Federacją Rosyjską i Republiką Białorusi. Należy przy tym podkreślić, że ingerencja w wybory podlega sankcji karnej na podstawie art. 249 Kodeksu karnego, jak również może być podstawą do nałożenia sankcji międzynarodowych.

W ramach Krajowego Systemu Cyberbezpieczeństwa, przy udziale Ministerstwa Cyfryzacji, podejmowane są działania mające zapewnić cyberbezpieczeństwo zbliżających się wyborów prezydenckich[1]. Z uwagi na to, że szczególnie wrażliwym polem dla wrogich działań są prywatna infrastruktura cyfrowa oraz media społecznościowe, niezwykle ważne są nie tylko działania instytucji publicznych, ale też sektora prywatnego, platform społecznościowych i wszystkich przedstawicieli społeczeństwa.

Jednym z zagrożeń są techniczne cyberataki związane z przełamaniem zabezpieczeń (w tym przy wykorzystaniu socjotechniki), które mogą być podejmowane w celu zakłócenia cyfrowej infrastruktury pośrednio powiązanej z procesem przeprowadzenia wyborów, jak również innych publicznych i prywatnych systemów informacyjnych, które adwersarze chcieliby zakłócić, aby osiągnąć efekt chaosu. Szereg polskich instytucji podejmuje działania, aby jak skuteczniej uniemożliwić tego rodzaju cyberataki.

Jak pokazują doświadczenia, celem cyberataków może stać się także infrastruktura cyfrowa, która zdawać by się mogło nie jest powiązana z procesami wyborczymi, jak np. kioski informacyjne w centrach handlowych. Dlatego kluczowe jest, aby administratorzy systemów stosowali zasady bezpieczeństwa, w szczególności w zakresie aktualizacji oprogramowania oraz dwuskładnikowego uwierzytelnienia. Ważne jest także upowszechnianie zasad higieny cyfrowej wśród wszystkich użytkowników, aby minimalizować ryzyka związane z socjotechniką.

[1] Instytucją wiodącą w zakresie zapewniania cyberbezpieczeństwa wyborów jest Agencja Bezpieczeństwa Wewnętrznego (ABW), zgodnie z jej ustawowymi kompetencjami określonymi w *ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* oraz *ustawie o krajowym systemie cyberbezpieczeństwa* (zadania zespołu CSIRT GOV prowadzonego przez ABW).

telefon: +48 22 245 59 22
adres email: sekretariat.dc@cyfra.gov.pl
adres strony internetowej: www.gov.pl/cyfryzacja

adres:
ul. Królewska 27
00-060 Warszawa

Kolejnym z rodzajów zagrożeń związanych z wyborami są wrogie operacje wpływu, w tym rozpowszechnianie dezinformacji, obliczone na pogłębianie polaryzacji społeczeństwa, kwestionowanie istoty demokracji oraz stworzenie braku pewności co do uczciwości wyborów i ich rezultatu. Kluczowa jest tutaj rola platform internetowych, aby skutecznie przeciwdziałały wykorzystaniu ich zasobów do operacji wpływu i dezinformowania oraz niezwłocznie usuwały tego rodzaju treści. Bezwzględnie będziemy wymagać należytej staranności w tym zakresie, stosowania odpowiednich przepisów prawa oraz współpracy z właściwymi podmiotami Krajowego Systemu Cyberbezpieczeństwa.

Zwracam się również do wszystkich obywateli o roztropność i refleksję przy dalszym udostępnianiu treści w mediach społecznościowych, które mogą być elementem wrogiej, sponsorowanej przez nieprzyjazne państwa, operacji wpływu i kampanii dezinformacyjnych. Państwo będzie aktywnie działało na rzecz zwalczania nielegalnych treści w internecie, ale my także jako obywatele weryfikujmy informacje w rzetelnych źródłach.

Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa