FUNDACJA IM. STEFANA BATOREGO

forumIdei

Głosowanie internetowe. Dlaczego nie teraz?

Maciej Broniarz, Tomasz Zieliński

Bezpieczeństwo i niezawodność systemów informatycznych pozostawiają wiele do życzenia. Nawet osoby, które potrafią korzystać ze smartfonów, komputerów i Internetu, padają ofiarami wyłudzeń i oszustw. Każdego dnia ujawniane są nowe incydenty związane z bezpieczeństwem w sieci – od zaszyfrowania zasobów firm znanych z pierwszych stron gazet przez wycieki danych operatorów usług medycznych aż do oszukańczych inwestycji w „pewny biznes z kryptowalutami". Osobną kategorię stanowią wreszcie politycy, których poufne maile od lat ujawniane są w sieci, łamiący zasady bezpieczeństwa w imię swoiście rozumianej konspiracji.

Powracający regularnie pomysł na głosowanie przez Internet udowadnia, że politycy wydają się nie rozumieć istoty problemu i skupiają się na przekazie o nowoczesności i cyfryzacji. Polska ma tu wiele do nadrobienia, ale proces wyborczy nie jest jednym z tych obszarów. Znacznie więcej i to ważniejszych innowacji musimy zrealizować, by podnosić efektywność np. ochrony zdrowia i wymiaru sprawiedliwości.

W takich oto okolicznościach po raz kolejny powraca pomysł głosowania przez Internet w wyborach powszechnych. Budując chociażby na wspomnianych wyżej doświadczeniach, możemy mieć duże i uzasadnione obawy co do wyboru takiej formy głosowania.

Zapytajmy na serio – po co komu wybory przez sieć?

Od wielu lat koronnym argumentem przemawiającym za głosowaniem przez Internet w wyborach powszechnych była – zdaniem wielu polityków – zbyt niska frekwencja. Możliwość zdalnego oddania głosu miałaby ją zwiększyć, automatycznie poprawiając jakość demokracji.

Wybory parlamentarne z 2023 roku, w których udział wzięło 74,38% uprawnionych, pokazały jasno, że wyborcy potrafią się zmobilizować i masowo ruszyć do urn – tym samym temat organizacji wyborów

przez Internet można zamknąć. W poniższych rozważaniach odchodzimy więc od pytania „po co?", skupiając się jedynie na kwestii „jak?" je zorganizować oraz jakie zagrożenia czyhają po drodze.

Wszyscy zgodzimy się chyba, że skoro wybory przez Internet nie przyniosą spektakularnych korzyści, nie powinniśmy iść na żadne kompromisy i godzić się tak na obniżanie poziomu ich wiarygodności, jak i na odejście od któregokolwiek z ustawowych przymiotów: powszechności, równości, bezpośredniości, proporcjonalności oraz tajności oddania głosu. Niemniej, te argumenty mogą nie trafiać do uszu decydentów.

Problem, który nie istnieje

Pandemia COVID-19 przyspieszyła cyfryzację wielu obszarów życia − w tym wyborów. Centralny Rejestr Wyborców wprowadzony przed wyborami parlamentarnymi w 2023 roku diametralnie uprościł głosowanie poza miejscem zamieszkania. Ten poziom cyfryzacji procesu wyborczego dowodzi, że narzędzia informatyczne ułatwiają udział w głosowaniu, bez konieczności wdrażania systemu oddawania głosu przez Internet.

Wykorzystywanie narzędzi informatycznych ma sens wtedy, gdy rozwiązuje konkretne problemy − *vide* wspomniany już Centralny Rejestr Wyborców. Należy unikać pokusy przenoszenia procesów do Internetu tylko po to, aby było nowocześnie. Takie podejście prezentują, niestety, rządzący, którzy w ten sposób chcą dowieść swojej (pozornej) nowoczesności, tymczasem wykazują się brakiem zrozumienia rzeczywistych problemów współczesnego społeczeństwa.

Jakie zagrożenia wiążą się z procesem wyborczym przeniesionym do Internetu? Dwie główne kategorie to zaburzanie procesu oddawania głosu i fałszowanie procesu liczenia głosów.

Ochrona procesu głosowania przez Internet

Klasyczne wybory to ponad 31 tysięcy obwodów wyborczych. Tak duże rozproszenie sprawia, że trudno zakłócić je w dużej skali. Inaczej mogłoby być podczas wyborów przez Internet. Tu sabotaż infrastruktury serwerowej wymaga znalezienia tylko jednego słabego punktu − a gdy go nie będzie, na podorędziu zawsze czeka przecież klasyczny DDOS (atak polegający na zalaniu serwerów taką liczbą żądań, której nie będą w stanie obsłużyć).

Kolejnym wyzwaniem może być sprzedaż głosów. W klasycznych wyborach ryzyko takie oczywiście istnieje, ale realizacja wiąże się dla kupującego z trudnościami logistycznymi i wystawia go na ryzyko ujawnienia tożsamości. Gdy jednak głos w wyborach można oddać w sieci, kupujący głosy zyska możliwość głosowania w cudzym imieniu lub przynajmniej nadzoru innej osoby (np. przez zdalny pulpit), przy jednoczesnym zachowaniu pełnej anonimowości.

W obecnym modelu wyborów nie można wziąć dowodu chorego członka rodziny i pójść zagłosować w jego imieniu. W przypadku głosowania elektronicznego jest to jak najbardziej możliwe. Osoby starsze lub mniej biegłe technologicznie często proszą młodszych o pomoc w przelewie online albo internetowym zapisie na szczepienie. W przypadku głosowania elektronicznego mogłoby być tak samo. W efekcie możliwe będzie głosowanie w imieniu kogoś innego i to bez uwzględnienia jego preferencji wyborczych.

Humorystyczne hasło „zabierz babci dowód" zamienia się tu w zupełnie nieśmieszne „odbierz babci głos". Nie wspominając już o rodzinach, w których jeden z członków dominuje nad pozostałymi i oczekuje, że będą oni stosować się do jego woli − również w zakresie wyborów politycznych.

Socjotechnika jest prostsza niż włam na serwer

Projekt systemu do e-głosowania będzie kompromisem między bezpieczeństwem procesu logowania a łatwością jego użycia. Może to w rezultacie stworzyć warunki do przejmowania cudzych kont do głosowania (np. poprzez ataki phishingowe lub socjotechnikę) oraz do kupowania dostępu do kont osób upoważnionych do głosowania. W obu przypadkach system do e-głosowania stwarza możliwość nadużyć, *de facto* nie rozwiązując żadnego z istotnych problemów.

Realizacja zdalnego głosowania przy użyciu fizycznego składnika uwierzytelniania, np. podpisu cyfrowego osadzonego w chipie dowodu osobistego, dramatycznie ograniczy liczbę osób potrafiących przeprowadzić taką operację. Z kolei wykorzystanie istniejących serwisów rządowych, np. Profilu − *nomen omen* − Zaufanego, może podkopać zaufanie obywatela do anonimowości tak oddawanego głosu.

Ochrona procesu liczenia głosów

Niezwykle istotną cechą klasycznego procesu wyborczego jest jego transparentność. Każda komisja wyborcza składa się z kilku osób, zaś rywalizujące ze sobą komitety delegują swoich przedstawicieli. Komisja po zliczeniu głosów wywiesza w widocznym miejscu protokół, każdy zainteresowany może go sobie sfotografować i porównać jego treść z liczbami prezentowanymi na stronach internetowych Państwowej Komisji Wyborczej.

Partie albo inne organizacje społeczne są w stanie samodzielnie zweryfikować prawidłowość liczenia głosów. Inicjatywy obserwatoriów wyborczych często i z powodzeniem działają w tym modelu, dając dodatkową gwarancję uczciwości i transparentności wyborów. W modelu głosowania elektronicznego taki mechanizm kontroli nie byłby możliwy.

Owszem, PKW używa własnego, dedykowanego oprogramowania, aby sumowanie przebiegało szybko i sprawnie, jednak w razie awarii technicznej wyniki można przedyktować przez telefon. Zawsze powstaje też papierowy protokół, przekazywany fizycznie do PKW przed ogłoszeniem wyników końcowych.

Gdy dopuścimy głosowanie przez Internet, proces taki będzie o wiele mniej transparentny. Tracimy możliwość społecznego audytu zliczania i sumowania głosów. Oczywiście, istnieją algorytmy dające głosującemu możliwość zweryfikowania, czy jego głos został zliczony poprawnie, przy jednoczesnym zachowaniu tajności/anonimowości. Stopień ich skomplikowania jest jednak tak duży, że ich użycie mija się z celem − prawie nikt nie potrafiłby samodzielnie przeprowadzić weryfikacji. Wchodzimy więc na drugi poziom absurdu − musimy zaufać komuś, kto zweryfikuje nam dane instytucji, której nie ufamy.

Dostęp do źródeł oprogramowania użytego w głosowaniu pozwoliłby, w najlepszym razie, sprawdzić, czy proces oddania głosu spełnia kryteria bezpośredniości i tajności, czy przekazywany zestaw informacji zawiera tylko konieczne elementy. Nigdy nie będziemy jednak pewni, co działa po drugiej stronie, w jaki sposób oprogramowanie serwerowe przetwarza otrzymane informacje.

Gdzie przypisać zdalny głos?

Głosowanie zdalne nie zastąpi głosowania klasycznego, rodzi się więc pytanie: jak zapobiec głosowaniu tej samej osoby przez Internet i w lokalu? Jedyna sensowna opcja to pobranie „wirtualnego zaświadczenia" i wykreślenie ze spisu wyborców w obwodzie.

Do którego obwodu zaliczyć wówczas taki głos? Pierwotnego? A może do warszawskiego obwodu nr 19, do którego wliczane są głosy z zagranicy? Bo chyba nikomu nie przyjdzie do głowy utworzenie „obwodu wirtualnego" na głosy z Internetu? Zasada proporcjonalności i równości wyborów byłaby jeszcze bardziej zagrożona.

Co w przypadku podejrzeń nieprawidłowości?

Kto walczył ze spamem, ten przekonał się, że przy wykrywaniu nadużyć online trudno o zerojedynkowość. Jeden głos oddany przez Internet z IP należącego do Zimbabwe nie wzbudzi zdziwienia, ale pięć takich głosów w kwadrans? A sto? Albo tysiąc?

Wiemy, że policja nie ma zasobów do szybkich interwencji w sferze wirtualnej, zwłaszcza w niedzielę wyborczą. Co zatem zrobić w sytuacji, gdy PKW będzie podejrzewać fałszerstwo? Kto i na jakiej podstawie podejmie decyzję o eliminacji wątpliwych głosów? I czy w ogóle da się to zrobić?

Jeśli system do głosowania oddzieli oddany głos od (uwierzytelnionego uprzednio) obywatela, a tak przecież być powinno, to stracimy możliwość poinformowania tego obywatela o unieważnieniu głosu lub o organizacji powtórzonego głosowania.

W jaki sposób audytować zrealizowane unieważnienia głosów? Jeśli nawet od strony technicznej oddzielimy tożsamość od głosów i zakodujemy głosy w sposób nieczytelny dla operatora, to metadane (np. numer IP albo pierwotny obwód wyborczy) przekładają się na tendencje statystyczne. Nieuczciwy admin może pomóc „swojej" opcji politycznej, unieważniając po cichu internetowe głosy z Podlasia lub centrum Warszawy.

Kryptografia jest trudna

Skąd zwykły człowiek wie, że współczesna kryptografia zapewnia odpowiedni poziom szyfrowania danych przesyłanych przez sieć komputerową? To proste − skoro banki dają klientom dostęp do rachunków przez Internet, to taka transmisja zapewnia dostateczną poufność (przesyłanych treści nie da się podejrzeć) oraz integralność (przesyłanych treści nie da się zmodyfikować).

W jaki jednak sposób można zyskać pewność, że szyfrowanie jest odporne na ataki? Nie każdy wyborca, a właściwie tylko niewielu z nich, jest w stanie pójść na studia matematyczne i informatyczne, by już po kilku semestrach algebry, matematyki dyskretnej, kombinatoryki i kryptografii... opanować pojęcia wymagane do nauki algorytmów szyfrowania rzeczywiście stosowanych w Internecie.

Kryptografia jest trudna. Co z tego, że istnieją algorytmy łączące anonimowość głosowania z weryfikowalnością poprawności zliczenia głosu, skoro rozumieć je będzie jeden procent głosujących? Pozostali będą musieli we wszystko uwierzyć: w to, że takie algorytmy istnieją, że faktycznie zostały użyte w wyborach, że zostały poprawnie zaimplementowane, że nikt nie pozostawił w kodzie testowej funkcji zapisującej do pliku informacji diagnostycznych i oddanych głosów wraz z danymi głosujących.

Kwestia zaufania

W istotę demokracji wpisane jest ograniczone zaufanie do procesu wyborczego. Partia rządząca zawsze będzie miała pokusę, by wykorzystać kontrolowane przez siebie instytucje państwowe w celu utrzymania władzy. Partia przegrywająca wybory zawsze będzie miała pokusę, by usprawiedliwiać porażkę oszustwami i fałszerstwami.

Im większa polaryzacja społeczeństwa, tym łatwiej znaleźć kogoś, kto dla korzyści własnego obozu politycznego nagnie lub złamie reguły prawa. Jeszcze ważniejsze staje się więc, aby w wyborach powszechnych jak największa część procesu głosowania była przejrzysta i jak najmniej zależało od działań małej grupy ludzi.

W klasycznych wyborach sfałszowanie ich wyniku wymagałoby przekupienia lub zastraszenia tysięcy ludzi pracujących w setkach komisji wyborczych. Wybory przez Internet wymagają od społeczeństwa stanowczo za dużo zaufania. Musimy ufać, że infrastruktura jest zabezpieczona przed nieautoryzowanym dostępem, że głosy zawsze zliczane są bezbłędnie, że niemożliwa będzie ich późniejsza modyfikacja, że raporty i protokoły odpowiadają wcześniej oddanym głosom i tak dalej.

Integralność infrastruktury w wielu miejscach będzie zależała od niewielkiej grupy osób. Jeśli choć jedna z nich zechce zobaczyć, jak płonie demokracja, to zdoła otworzyć system informatyczny na ataki z zewnątrz, posługując się działaniami wyglądającymi na niewinną pomyłkę w codziennej pracy.

Cały proces głosowania przez Internet będzie się na jakimś etapie opierał na niemal ślepym zaufaniu, zaś rezultat wyborów wpłynie także na tych, którzy wyborom przez Internet ufać nie chcą.

Co będzie, gdy anarchizujący polityk zacznie przekonywać, że wybory przez Internet to spisek, a rząd widzi, kto i jak głosował? Ilu profesorów matematyki potrzeba, aby przegadać takiego polityka w programie telewizyjnym?

Oszczędności nie będzie

Według niektórych źródeł[1] wybory parlamentarne w 2023 roku mogły kosztować ponad 300 mln zł. Wybory przez Internet znacząco zwiększą tę kwotę. Dlaczego?

Po pierwsze, potrzebna będzie nowa infrastruktura serwerowa i sieciowa. Regularnie doświadczamy przeciążenia Profilu Zaufanego, e-PIT czy Internetowego Konta Pacjenta, a przecież systemy te towarzyszą nam od wielu lat. System do elektronicznych wyborów musiałby być przygotowany z jeszcze większym zapasem mocy − to koszt wielu milionów złotych.

Po drugie, oprócz kosztów przygotowania oprogramowania, będziemy musieli ponosić regularne koszty jego modernizacji i adaptacji. Utrzymanie i testowanie systemu, który zostanie użyty raz w roku lub rzadziej, będzie wymagało dosypywania pieniędzy przed każdym takim wydarzeniem. Czy na pewno zechce to zrobić siła polityczna, której nie sprzyjają wyborcy internetowi?

Po trzecie, najprostszym sposobem na podniesienie frekwencji jest ułatwienie udziału w głosowaniu. Zamiast ponosić koszty produkcji i utrzymania systemów IT, możemy wydać pieniądze na pomoc

1 J. Frączyk, *Za te wybory zapłaci każdy z nas. Gigantyczna kwota*, „Business Insider", 8 sierpnia 2023, https://businessinsider.com.pl/polityka/za-te-wybory-zaplaci-kazdy-z-nas-gigantyczna-kwota/84v1qyt [dostęp: 28.05.2024].

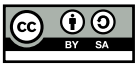
osobom, które nie są w stanie samodzielnie dotrzeć do punktu głosowania. Tu państwo ma wiele do nadrobienia.

Jakie byłyby rzeczywiste oszczędności w głosowaniu przez Internet? Liczba obwodów wyborczych zależy od decyzji politycznej, więc tych kosztów nie liczymy. Jeśli zdalnie zagłosowałoby 2% uprawnionych (tyle, ile w roku 2023 głosowało poza miejscem zamieszkania), zaoszczędzimy około 300 tys. zł na kosztach druku niepotrzebnych kart wyborczych. A to akurat roczna pensja jednego specjalisty z branży IT.

Maciej Broniarz – od 1998 roku administrator systemów IT. Związany zawodowo z Uniwersytetem Warszawskim, wykładowca na Wydziale Matematyki, Informatyki i Mechaniku UW, ekspert Centrum Nauk Sądowych z zakresu bezpieczeństwa IT w zakresie informatyki kryminalistycznej. Architekt systemów IT i audytor bezpieczeństwa. Zrealizował kilkaset projektów IT – od małych wdrożeń po systemy przeznaczone dla setek tysięcy użytkowników. Współpracownik Polskiego Towarzystwa Kryminalistycznego w zakresie bezpieczeństwa IT. Ekspert ds. bezpieczeństwa IT, computer forensics i Computer Security Incident Response.

Tomasz Zieliński – zawodowy programista od 2003 roku, pasjonat bezpieczeństwa informatycznego, autor bloga Informatyk Zakładowy. Rozwijał systemy finansowe dla NBP, tworzył i weryfikował zabezpieczenia bankowych aplikacji mobilnych, brał udział w pracach nad wyszukiwarką internetową Microsoft Bing. Obecnie pracuje w firmie DeepL.

Fundacja im. Stefana Batorego
Sapieżyńska 10a
00-215 Warszawa
tel. (48-22) 536 02 00
fax (48-22) 536 02 20
batory@batory.org.pl
www.batory.org.pl



Redakcja: Agnieszka Łodzińska
Korekta: Izabella Sariusz-Skąpska
Warszawa 2024
ISBN 978-83-67750-94-3