Bezpieczeństwo zliczania zbiorczych wyników głosowania

Raport Obserwatorium Wyborczego

30 września 2022

Niniejszy raport jest owocem obserwacji przeprowadzonej 25 września br. podczas drugiej tury wyborów prezydenta Rudy Śląskiej. Opisane tu problemy są reprezentatywne dla wszelkiego rodzaju wyborów powszechnych w Polsce, gdyż procedura obliczania zbiorczych wyników wyborów (ang. *tabulation*; polskie określenie ustawowe, które pochodzi jeszczez PRL: *ustalanie wyników głosowania i wyników wyborów*) jest co do zasady zawsze niemal taka sama, nie zależy od rodzaju wyborów.

Pozostałe raporty Obserwatorium Wyborczego z wyborów przeprowadzonych 11 i 25 września br. w Rudzie Śląskiej:

- Przedterminowe Wybory Prezydenta Rudy Śląskiej, 11 września 2022. Raport po pierwszej turze https://ow.org.pl/2022/09/12/przedterminowe-wybory-prezydenta-rudy-slaskiej-11-09-2022-raport-po-pierwszej-turze/
- Przedterminowe Wybory Prezydenta Rudy Śląskiej. Druga tura, 25 września 2022. Raport https://ow.org.pl/2022/09/30/przedterminowe-wybory-prezydenta-rudy-slaskiej-druga-tura-25-wrzesnia-2022-raport/

Nasze wnioski: Prawidłowe obliczenie zbiorczych wyników głosowania uzależnione jest od poprawnego działania informatycznego systemu wsparcia wyborów (WOW), który jest zabezpieczony przed prostymi atakami, ale podatny na ataki bardziej wyrafinowane.

Ważnym środkiem ochrony systemu obliczania wyników przed atakami jest pełne ogłaszanie danych z wyborów: wywieszanie papierowych protokołów przez obwodowe komisje wyborcze i publikowanie w internecie elektronicznych wersji tych protokołów. Zdaniem Obserwatorium Wyborczego, ta ochrona wymaga wzmocnienia przez dodatkowe działania, a mianowicie:

- Każdej wersji każdego protokołu obwodowej komisji wyborczej powinna być publikowana w internecie, gdy tylko została wprowadzona do systemu, a więc zanim jeszcze została w jakikolwiek sposób zatwierdzona czy choćby wydrukowana w wersji papierowej (w szczególności wersje protokołu, które nigdy nie zostaną zatwierdzone, gdyż zawierają błędy, też powinny być publikowane);
- Członkowie obwodowych komisji wyborczych powinni być zobowiązani do sprawdzania, czy wyniki z ich komisji opublikowane w internecie są zgodne z ich papierowymi protokołami.

Waga problemu

Ewentualne ataki informatyczne na administrację wyborczą mogą pochodzić z Polski lub z zagranicy. Takie ataki mogą nawet pochodzić z wewnątrz organów wyborczych (sabotaż systemu przez osoby, których zadaniem jest jego rozwijanie i wspieranie). Celem ataku może być nieuczciwa zmiana wyników wyborów lub też wprowadzenie zawirowań, które zdezorganizują pracę komisji wyborczych, spowodują opóźnienia w obliczaniu wyników i będą pretekstem do podważenia wiarygodności wyników w oczach obywateli.

Zmiana wyniku wyborów przy pomocy takiego ataku jest stosunkowo trudna ze względu na już istniejące środki ochrony, o których poniżej, natomiast dezorganizacja pracy komisji wyborczych wydaje się być dziś w zasięgu ręki osób, które mają złe intencje, o ile tylko osoby te mają odpowiednie umiejętności. Tego typu dezorganizacja oraz wynikające z niej opóźnienia w pracy organów wyborczych miały miejsce podczas wyborów samorządowych w roku 2014. Spowodowały, że wiarygodność organów wyborczych była publicznie podważana, co zaowocowało dymisją prawie wszystkich członków Państwowej Komisji Wyborczej (PKW) (wówczas źródłem problemu były błędy w systemie informatycznym Krajowego Biura Wyborczego (KBW), nie było ataku na ten system). W tym samym roku na Ukrainie autor niniejszego raportu był, jako obserwator OBWE, świadkiem podobnych zawirowań, ale na mniejszą skalę (opóźnienie pracy komisji wyborczych różnych szczebli wynoszące kilka godzin i powodujące nadzwyczajne przemęczenie wielu członków komisji; wówczas jako przyczynę podawano ataki informatyczne).

Wyniki wyborów powinny być obliczane w sposób w miarę możności odporny na takie problemy. Jest to kwestia techniczna, która ma duże konsekwencje polityczne i wpływ na wiarygodność państwa polskiego.

Jak są obliczane zbiorcze wyniki głosowania

Obwodowe komisje wyborcze tworzą swoje protokoły na komputerach osobistych (tzw. PCtach), przy pomocy oprogramowania WOW (Wsparcie Organów Wyborczych). Każdy taki protokół jest wysyłany przez internet do serwerów Krajowego Biura Wyborczego (KBW), a stamtąd wyniki pobiera komisja wyższego rzędu, która oblicza wyniki zbiorcze. W Rudzie Śląskiej komisją wyższego rzędu była miejska komisja wyborcza, w różnego rodzaju wyborach są to komisje terytorialne (gminne, miejskie, powiatowe i wojewódzkie), sektorowe i okręgowe oraz PKW. Protokół komisji obwodowej utworzony na komputerze przy pomocy WOW jest drukowany, a następnie podpisywany przez wszystkich członków komisji obwodowej.

Komisja wyższego rzędu oblicza zbiorcze wyniki głosowania na podstawie tego, co otrzymała przez internet. **Komisja nie porównuje treści protokołów otrzymanych przez internet z protokołami papierowymi; treści protokołów papierowych nikt nie czyta w całości: w najlepszym razie ktoś czyta niektóre dane, w najgorszym nikt nic nie czyta.**

W wyborach w Rudzie Śląskiej najważniejsze dane (który kandydat dostał ile głosów) były spisywane przez członków komisji miejskiej z protokołów papierowych do tabelek na papierze, ale innych danych (np. liczba głosów nieważnych) w ogóle nikt nie czytał w protokołach papierowych.

Zgodnie z wytycznymi PKW, komisja wyższego rzędu sprawdza jedynie, czy protokół na papierze i protokół wysłany przez internet mają taki sam *symbol kontrolny*. Jeśli symbol kontrolny się zgadza,

to komisja uznaje, że protokół wysłany przez internet zawiera dane identyczne z tymi zawartymi w protokole na papierze i dalej używa protokołu wysłanego przez internet.

Symbol kontrolny, to unikalny identyfikator, który WOW przypisuje każdej wersji każdego protokołu: jeżeli w danej komisji obwodowej sporządzono kilka kolejnych wersji protokołu (co zdarza się, jeśli trzeba poprawiać błędy), to każda wersja ma inny symbol kontrolny.

Podsumowując: członkowie komisji obwodowych podpisują protokół na papierze zawierający wyniki głosowania i symbol kontrolny, ale potem nikt nie ma obowiązku patrzeć (i często nikt nie patrzy) na wyniki głosowania, jedynie symbol kontrolny ma znaczenie. Gdyby członkowie komisji podpisywali jedynie symbol kontrolny na małej kartce, a w ogóle by nie podpisywali ani nawet nie drukowali protokołu na papierze, to z punktu widzenia komisji wyborczej wyższego rzędu efekt byłby taki sam.

Przed czym system jest zabezpieczony

W systemie informatycznym wspierającym wybory prowadzone są w szczególności następujące działania:

1. informatyk komisji obwodowej wprowadza do komputera, który znajduje się w komisji, dane, które mają być zawarte w protokole;
2. komputer znajdujący się w komisji obwodowej wyświetla te dane na ekranie – członkowie komisji, mężowie zaufania i obserwatorzy są uprawnieni, by je oglądać;
3. komputer znajdujący się w komisji obwodowej drukuje na papierze protokół zawierający te dane i symbol kontrolny;
4. komputer znajdujący się w komisji obwodowej wysyła te dane przez internet do serwerów KBW; dane są powiązane nas serwerach z symbolem kontrolnym;
5. te dane są następnie brane pod uwagę przez serwery KBW przy obliczaniu zbiorczych wyników wyborów.

Jeżeli ten system działa prawidłowo (w szczególności: dane, o których mowa w punktach od 1 do 5 powyżej, są takie same), to taki sposób procedowania jest bezpieczny, a symbol kontrolny daje pewność, że to, co podpisali członkowie komisji obwodowej, jest tożsame z danymi, na podstawie których obliczany jest wynik głosowania.

Ten system jest zabezpieczony przed stosunkowo prostymi atakami. Na przykład jeśli ktoś ukradnie hasło, które pozwala komisji obwodowej logować się w WOW, i dzięki temu wprowadzi fałszywy protokół do systemu, to sprawdzenie symbolu kontrolnego pozwoli wykryć takie oszustwo: protokół wprowadzony przez oszusta będzie miał inny symbol kontrolny niż protokół papierowy podpisany przez komisję obwodową.

Na co system jest podatny

System jest jednak podatny na ataki. Skoncentrujmy się na jednym rodzaju ataku, a mianowicie na hipotetycznym *fałszywym kliencie WOW*, czyli na oprogramowaniu, które by wyglądało jak ta część WOW, która działa na komputerze komisji obwodowej, i działałoby z pozoru tak samo, ale

nieuczciwie: fałszywy klient WOW przekazywałby przez internet do serwera KBW dane inne niż te, które są wprowadzane przez informatyka, wyświetlane na ekranie i drukowane: wówczas dane z punktów 1, 2 i 3 powyżej byłyby inne niż dane z punktów 4 i 5. W takim przypadku dane, na podstawie których obliczans są zbiorcze wyniki głosowania, byłyby inne niż dane w protokole na papierze.

Ataki przy pomocy fałszywego klienta WOW są możliwe do przeprowadzenia, gdyż komputery używane przez obwodowe komisje wyborcze, to zwykłe komputery należące do rozmaitych gminnych instytucji (atak na serwery KBW byłby trudniejszy, o ile KBW działa zgodnie z zasadami sztuki). Fałszywego klienta WOW można wprowadzić do komputera komisji obwodowej na kilka sposobów: może to zrobić nieuczciwy serwisant, można przez manipulację psychologiczną nakłonić prawowitego użytkownika komputera, żeby to zrobił nieświadomie (np. „konieczna jest aktualizacja sterownika drukarki” – a w rzeczywistości to nie sterownik, tylko fałszywy klient WOW), można także rozprowadzać wirus, który będzie to robić.

Działanie fałszywego klienta WOW byłoby nie do wykrycia przez członków komisji obwodowej, mężów zaufania i obserwatorów, którzy przyglądają się tworzeniu protokołu z komisji. Byłoby też trudne do wykrycia przez informatyka, który obsługuje komisję.

Jak system jest chroniony dziś

System, który obecnie chroni wybory przed atakami informatycznymi na WOW, działa następująco: każda obwodowa komisja wyborcza wywiesza swój protokół na papierze, a następnie KBW publikuje w internecie treść wszystkich protokołów otrzymanych przez internet i zbiorcze wyniki głosowania obliczone na ich podstawie. Dzięki temu każdy może sprawdzić dwie rzeczy:

- czy papierowe protokoły wywieszone przez komisje obwodowe są identyczne z tym, co KBW otrzymał przez internet i publikuje w internecie;
- oraz czy zbiorcze wyniki wyborów są poprawne biorąc pod uwagę treść protokołów opublikowaną w internecie.

W sumie możliwe jest pełne sprawdzenie poprawności działania systemu, przy czym nie ma potrzeby, aby jedna osoba lub organizacja sprawdzała wszystko: niektóre osoby mogą sprawdzać dla poszczególnych obwodów głosowania zgodność danych w internecie z wywieszonymi protokołami papierowymi, kto inny może sprawdzić, czy zbiorcze wyniki są prawidłowo obliczone na podstawie danych opublikowanych w internecie.

Ten system sprawdzania poprawności wyników jest w teorii doskonały (chroni nas przed wszelkimi atakami na WOW lub błędami w WOW), w praktyce ma jednak dwa poważne niedostatki.

Po pierwsze, takie sprawdzanie wyników opiera się na niemałym wysiłku wolontariuszy (zbieranie danych z wywieszonych protokołów jest pracochłonne). Podczas wyborów wolontariusze są przeciążeni pracą (na przykład funkcją obserwatora społecznego) i opieranie się na nich, aby sprawdzić, czy system WOW działa prawidłowo, nie jest właściwe.

Po drugie, takie sprawdzanie wyników daje efekt w najlepszym razie z kilkugodzinnym opóźnieniem. W przypadku poważnych problemów z WOW, które mogą skutkować nawet

konieczności zliczania wyników w inny sposób (np. w arkuszu kalkulacyjnym stworzonym ad hoc na podstawie papierowych protokołów), kilkugodzinne opóźnienie byłoby bardzo szkodliwe.

.

Jak wzmocnić ochronę systemu

Proponujemy dwa środki zaradcze w odpowiedzi na problemy opisane powyżej.

Po pierwsze, serwery KBW powinny publikować w internecie jak najszybciej (najlepiej w ciągu kilku sekund) każdą wersję każdego protokołu z komisji obwodowej, która została wprowadzona do systemu (jeśli jakaś komisja wyborcza wprowadziła wiele wersji z powodu błędów wykrywanych w kolejnych wersjach, wszystkie te wersje powinny być widoczne). Każda wersja powinna być publikowana wraz z symbolem kontrolnym i ze statusem. Status, to może być w szczególności:

- wersja wprowadzona przez informatyka komisji obwodowej, ale na razie niepodpisana;
- wersja podpisana przez członków komisji obwodowej;
- wersja wstępnie zweryfikowane przez komisję wyższego rzędu po porównaniu z protokołem podpisanym na papierze;
- wersja definitywnie zaakceptowana przez komisję wyższego rzędu
- wersja odrzucona przez komisję wyższego rzędu

Taka publikacja pozwoliłaby członkom obwodowej komisji wyborczej, mężom zaufania i obserwatorom na porównywanie wersji papierowej, która została wydrukowana i jest w trakcie podpisywania, z tym, co jest na serwerach KBW. Do weryfikacji każdy mógłby używać swojego telefonu lub dowolnego komputera. Członek komisji obwodowej mógłby zastrzec, że nie podpisze protokołu papierowego, póki nie zobaczy na serwerach KBW protokołu o identycznej treści, z identycznym symbolem kontrolnym. Mógłby też podpisać protokół bez takiej weryfikacji, ale dokonać weryfikacji w kolejnych minutach i, w przypadku wykrycia rozbieżności, wszcząć alarm.

Podstawową korzyścią z takiego systemu byłaby całkowita ochrona przed fałszywym klientem WOW: ten system pozwala każdemu porównywać protokół papierowy z tym, co zostało wysłane do serwerów KBW, a więc gdyby fałszywy klient WOW coś sfałszował i wysłał nie to, co trzeba – taka sytuacja zostanie wykryta.

Drugą korzyścią byłaby realna możliwość weryfikacji protokołów przez każdego członka komisji, męża zaufania i obserwatora, w tym weryfikacji szczegółowej. Przy obecnym systemie, możliwość weryfikacji teoretycznie jest, ale w praktyce nie zawsze dobrze działa. Protokół w wersji elektronicznej pojawia się bowiem tylko na jednym ekranie komputera. Członkowie komisji (nierzadko w liczbie 11), mężowie zaufania i obserwatorzy w teorii mają prawo na ten ekran patrzeć, ale w praktyce niekoniecznie mogą to robić w komfortowych warunkach (jest za dużo osób). Niekoniecznie mają czas, żeby wszystko dokładnie obejrzeć: ani nie są uprawnieni, żeby żądać spowolnienia działań (dłuższego wyświetlanie danych), ani atmosfera nie jest korzystna dla osób, które prosiłyby o jakiekolwiek spowolnienie (wszyscy są przepracowani i niewyspani, chcą jak najszybszego zakończenia pracy).

Trzecią korzyścią byłoby umożliwienie osobom postronnym weryfikacji wywieszonego protokołu w każdym czasie: przy obecnym systemie protokół papierowy świeżo wywieszony przez obwodową komisję wyborczą dopiero po pewnym czasie (zazwyczaj po kilku godzinach) zostanie opublikowany w wersji elektronicznej. Póki nie jest opublikowany, osoby postronne go mogą fotografować lub robić notatki w celu późniejszej weryfikacji, ale nie mogą po prostu od razu dokonać weryfikacji.

Po drugie, członkowie obwodowych komisji wyborczych powinni być instruowani, że mają porównywać protokoły papierowe w swoim posiadaniu z tym, co KBW publikuje w internecie. Ten dodatkowy obowiązek powinien wiązać się z nieznacznym zwiększeniem diet, jakie otrzymują członkowie komisji. Innymi słowy, wysiłek, który dziś robią wolontariusze, powinien stać się zadaniem członków komisji wyborczych.

Obserwatorium wyborcze https://ow.org.pl info@ow.org.pl tel. 883 188 969

Autor sprawozdania: *Marcin Skubiszewski*