Voto Electrónico, 2012

¿Cómo vamos?

Escucho el clamor de nuestros lectores, después de un proceso electoral más y de haber soportado nuevamente meses de saturación de candidatos en los medios. Sin embargo, este es el momento justo para analizar una importante parte del proceso electoral en la cual los desarrolladores de software, expertos en seguridad y administradores de sistemas podemos ejercer influencia sobre el rumbo que sigue el país y darnos el lujo de ignorar nuestro rol de profesionales hablaría muy mal de cada uno de nosotros. Es así que presento esta actualización del estado y reflexión acerca de lo que puede esperarle a nuestro país de avanzar las propuestas de adopción del voto electrónico.

Los lectores asiduos de SG podrán recordar que abordamos ya este tema en el número 27 (febrero del 2010) [1]. Desde entonces, tuve oportunidad de participar en algunas publicaciones [2] en las que expliqué los puntos básicos acerca de por qué toda implementación que pueda hacerse de voto electrónico, sin importar las mejores intenciones o incluso la pericia técnica del proveedor, no hay manera de que ésta resulte más confiable y garantice mejor cuidado de los derechos del votante que una revisión hecha por humanos de votos emitidos en papel.

Urnas electrónicas

Cuando nos hablan del voto electrónico, casi siempre pensamos directamente en las urnas electrónicas, estaciones de propósito específico diseñadas y configuradas para recibir directamente cada uno de los votos de los electores. Sus proponentes argumentan a su favor tres razones principalmente: reducción de costos, tiempo de entrega de resultados y mayor confiabilidad en el proceso. Estos tres puntos, como lo explico en los artículos citados anteriormente, se vienen abajo incluso ante una revisión somera del tema.

En México, el tema de las urnas electrónicas no nos resulta nuevo. Los primeros intentos fueron pilotos limitados en el Distrito Federal, en el año de 2003, y en Coahuila en 2005, para las elecciones locales. En ambos casos, las urnas fueron desarrolladas en casa y aplicadas a muy pequeña escala.

Para Coahuila, en 2008 la experiencia se repitió en 11 municipios. Las urnas se emplearon en 10 de ellos, pero en San Buenaventura, los partidos PAN, PANAL y PT impidieron su implementación dado que argumentaron podría resultar fraudulenta[3].

Una muy extraña característica del voto en Coahuila es que, para "asegurar" que todos los votos correspondieran con la voluntad ciudadana, los votantes tenían que emitirlo por vía electrónica y firmar el comprobante emitido por la urna, depositándolo en una segunda urna para el eventual caso de un recuento. Esto, obviamente, viola el principio de la secrecía del voto y permite el control corporativo o la compra del voto.

En el Distrito Federal, tras años de aparente silencio, el Instituto Electoral local (IEDF) intentó implementar urnas electrónicas de manufactura industrial. Tras haber firmado contrato con la empresa Pounce Consulting para la adquisición de 1000 urnas electrónicas, a mediados de abril tomó la decisión de rescindirlo[4] por demoras injustificables en la entrega de los equipos, así como por 28 fallas como: ensamblados incompletos, chapas trabadas, ranuras abiertas en el depósito de votos, micas transparentes, puertos extraíbles sin protección, compartimiento del cable sin tapa. En este caso, lo destacable es que aunque grupos de académicos de la UNAM y el IPN localizaron estas 28 fallas, lo que verdaderamente detuvo la implementación fue la demora en la entrega de los equipos. Así que es muy probable que el IEDF continuará intentando implementar urnas electrónicas.

Por último, veamos el caso de Jalisco: El Instituto Electoral y de Participación Ciudadana (IEPC) aprobó que para la votación local se empleen urnas electrónicas en los distritos 1 y 17 y en el municipio de Gómez Farías, para un 11% del padrón total. Tras una licitación muy cuestionada[5] la empresa ganadora fue también Pounce Consulting. En este caso, al igual que en el DF, la empresa demoró la entrega de las urnas en casi seis semanas, apenas entregando a tiempo cuando ya se analizaba la cancelación del contrato.

Previo a la elección, se realizaron cinco simulacros para presentar la urna a la población y para ir corrigiendo los problemas que presentaran, dentro de los cuales al que más seguimiento se le dio fue al que afectaba la secrecía del voto (podía verse el testigo impreso de los votantes anteriores). Las variaciones eléctricas causaron, al menos en una ocasión, impresión descontrolada de votos y en los simulacros se han reportado urnas pre-cargadas[6].

El modelo de urna empleado en Jalisco incluye no sólo el acopio de la votación, sino la transmisión de los resultados por vía de telefonía celular a las cabeceras distritales. Esto, si bien está protegido por criptografía, abre nuevas vías de ataque: No sólo cada una de las urnas se conecta a la red celular (aunque sea sólo por breves instantes), sino que los equipos centrales deben estar a la escucha. Esto permite no sólo un

Gunnar Wolf es administrador de sistemas para el Instituto de Investigaciones Económicas de la UNAM y desarrollador del proyecto Debian GNU/Linux.
http://gwolf.org

››"Darnos el lujo de ignorar nuestro rol de profesionales hablaría muy mal de cada uno de nosotros."

ataque que comprometa el sentido de los votos emitidos, sino que abre la puerta a ataques de negación de servicio.

Un problema reportado en cerca del 20% de las urnas fue, precisamente, la falta de cobertura celular. El distrito 1 de Jalisco cubre la parte norte del estado, una zona de profundas barrancas y de una gran cantidad de poblados de muy difícil acceso, los cuales no tienen cobertura de telefonía celular. El planteamiento de realizar las votaciones con urnas que contemplan la transmisión de datos por esta vía no sólo revela una profunda desconexión respecto a la población objetivo a cubrir, sino que, al presentar distintas vías para que se lleve a cabo el acopio de la información abre un vector más para el ataque, ya no tanto técnico sino a través de la ingeniería social.

Un punto alarmante de la implementación en Jalisco es el traslado de la figura legal de lo que constituye un voto. Si bien las urnas empleadas emiten testigos para asegurar la posibilidad de un recuento (cabe mencionar, no es universalmente aceptado que esto sea garantía suficiente), el documento de validez legal no es el papel testigo sino el estado interno de la memoria de la urna electrónica. En caso de presentarse un recuento, citando al consejero electoral Carlos Martínez Maguey: "existe la posibilidad de que se puedan contar los testigos de voto, no es vinculante el resultado del testigo de voto, pero siempre nos dará el mismo resultado que la base de datos". Los votos están en la memoria, y el papel únicamente da fe de ello. Esto significa que en Jalisco se ha legalizado la desmaterialización del voto. Y si bien el proceso electoral mexicano todavía da para muchas impugnaciones, hay reportes de inconsistencias[7] entre el número de votantes del IFE y del IEPC en la misma casilla.

Voto no presencial

Como sabemos, existe una gran cantidad de mexicanos que residen en el extranjero y un porcentaje importante se encuentra en una situación de precariedad legal por lo que no pueden registrarse como residentes legales o desplazarse libremente en su país de residencia. Así que el modelo que requiere registrarse y desplazarse hasta una embajada o consulado no aplica para ellos. Se han planteado dos modalidades para realizar el voto no presencial: El voto en línea y el voto postal.

Antes de analizar estas alternativas, es muy importante explicitar a lo que renunciamos con ambas: perdemos la garantía de que el votante sea verdaderamente quien dice ser. En caso del voto postal, es bastante probable que el votante correcto reciba el paquete con las boletas en la dirección indicada, pero mantiene la necesidad de registrar una dirección postal permanente, lo cual rompe con el planteamiento de origen.

En el caso del voto electrónico, la perspectiva es peor aún, porque si bien el potencial elector podría registrarse presentando los datos de su credencial electoral, las instrucciones y contraseña le son enviadas por correo electrónico. La confiabilidad y la confidencialidad de los proveedores de servicios de correo electrónico, especialmente de los gratuitos (que son por mucho los más frecuentemente utilizados) no garantizan que sea genuinamente el votante quien los revisa, especialmente en el caso de la población con menor dominio de la tecnología.

Lo que es más: En un escenario como el ampliamente impugnado en las elecciones recién ocurridas, la compra de votos se vuelve trivial. Basta con que el votante entregue su contraseña en los días previos al operador electoral y que éste verifique el poder votar por su propio partido, para la entrega de los recursos económicos.

En una plática informal con personal del IEDF, me indicaron estar al tanto de esta realidad, pero dada la cantidad de población registrada era un riesgo aceptable: Para este año, hubo 10,786 empadronados los cuales corresponden únicamente el 0.13% del padrón, pese a la grandísima campaña en medios. De ellos, apenas 4192 optaron por hacerlo en línea.

Conclusiones

Si bien he definido mi postura al respecto desde hace tiempo, he buscado expertos en seguridad en cómputo independientes (no asociados con empresas vendedoras de sistemas del rubro) dispuestos a argumentar a favor del voto electrónico, y honestamente no he encontrado a ninguno. Sin embargo, el voto electrónico tiene un atractivo desde un punto de vista político y hay un gran negocio en ofrecer soluciones basadas en él. Nosotros, como profesionales del ramo, más que buscar la oportunidad de negocio espero sepamos responder con los argumentos que hacen del voto electrónico un verdadero peligro para la democracia.

Los vendedores de urnas tienden a argumentar que ha habido elecciones exitosas con voto electrónico y justifican los fracasos indicando que fueron fallos puntuales de implementación. Sin embargo, mi punto es que es precisamente imposible hacer una implementación tan segura y confiable como lo que plantean reemplazar.

En una prueba piloto, o incluso en una primera implementación, es muy poco probable que se presente un ataque. En ambos casos, estaríamos hablando de implementaciones muy controladas, en que prácticamente si se registra una falla es por un error más que por un ataque.

Desde hace algunos meses hemos estado alimentando al Observatorio del Voto Electrónico[8]. Invito a los interesados a emplearlo como fuente de información, y a unirse a nuestro trabajo de análisis y difusión.

››Por Gunnar Wolf

Referencias:

[1] *"Voto electrónico, analizando su conveniencia".* http://swgu.ru/sg37r6
[2] *"Voto electrónico, ¿quien tiene realmente la decisión?"* http://swgu.ru/sg37r7
[3] *"Suspenden voto digital en San Buenaventura".* http://swgu.ru/sg37r8
[4] *"Urnas electrónicas tienen 28 fallas".* http://swgu.ru/sg37r9
[5] *"Notas de una escandalosa licitación que arriesga el voto electrónico".* http://swgu.ru/sg37r10
[6] *"Todavía es viable aplicar el voto electrónico en el estado".* http://swgu.ru/sg37r11
[7] *"El IEPC desmiente irregularidades en votación electrónica de distrito 1".* http://swgu.ru/sg37r12
[8] Observatorio del voto electrónico. http://evoto.iiec.unam.mx