

Nowe dziury w komputerach do e-votingu

<http://ipsec.pl/nowe-dziury-w-komputerach-do-e-votingu.html>

Audyt trzech amerykańskich komputerów do głosowania wykonany przez Uniwersytet Kalifornijski na zlecenie sekretarza tego stanu ujawnił szereg dziur i podatności w urządzeniach firm Sequoia, Diebold i HART.

http://www.sos.ca.gov/elections/elections_vr.htm > "University of California E-voting Report" < /a > opublikowany przez Uniwersytet jest wynikiem badania przeprowadzonego metodologią i testem penetracyjnym gora.

Badanie ujawniło szereg dziur i podatności w urządzeniach posiadających wydane wcześniej certyfikaty niezależnych laboratoriów, które są obowiązkowe dla komputerów wyborczych w USA. Były to dziury następujących rodzajów:

• możliwość podmiany oprogramowania (firmware) lub instalacji koni trojańskich za pomocą tak prostych środków jak U3 USB; podmiana była możliwa np. za pomocą spreparowanych plików z fontami (Sequoia), dziur w Windows (Diebold) czy nieudokumentowanego konta (Hart) • dziury umożliwiające zmianę wyników poszczególnych głosów lub oddawanie nieuprawnionych głosów (Sequoia) • wykonywanie nieautoryzowanych operacji, które nie były logowane w rejestrach bezpieczeństwa (Diebold) • stosowanie łatwych do zgadnięcia lub stałych, zaszytych w oprogramowaniu kluczy kryptograficznych (Diebold) • możliwość uzyskania nieautoryzowanego dostępu do wnętrza urządzenia, a w konsekwencji podmiana oprogramowania lub np. reset bez pozostawiania śladów (Diebold) • wszystkie testowane systemy były w praktyce oparte o Windows oraz standardowe oprogramowanie bazodanowe (jak np. MSDE), często bez aktualizacji i podstawowego hardeningu co otwiera te systemy na dziury odkryte w tych systemach do tej pory, lub takie, które zostaną odkryte w przyszłości - w systemie Hart możliwe było np. zdalne podsłuchiwanie tego co dzieje się w lokalu wyborczym

Badacze wskazali także na problemy organizacyjne związane z prowadzeniem testów - np. opóźnienia lub odmowę udostępnienia części oprogramowania przez poszczególnych producentów.

{Raport:

http://www.sos.ca.gov/elections/elections_vr.htm > University of California E - voting Reports < /a >

{Komentarze:

<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/07/28/VOTING.TMP> • "Most vote machines lose test to hackers" /a, SfGate.com • <http://www.pcworld.com/article/id,135199-page,1/article.html> • "California Report Slams E-Voting System Security" /a, PcWorld

Warto także zobaczyć co napisałem na <http://www.securitystandard.pl/> • SecurityStandard.pl/a o <http://blog.securitystandard.pl/news/118832.html> • zwycięstwie protokołu Punchscan w konkursie VoComp/a.