

O bezpieczeństwie "nowych" e-Deklaracji

<http://ipsec.pl/firmy/2009/o-bezpieczenstwie-quotnowychquot-e-deklaracji.html>

W wypowiedzi dla portalu Gazeta.pl koledzy z Securitum "na szybko" ocenili bezpieczeństwo serwisu e-Deklaracje. Jest to dobry argument, że słowa "bezpieczeństwo" i "na szybko" nigdy nie powinny występować w jednym zdaniu.

Jeśli chodzi o dostępność strony e-Deklaracje po SSL to częściowa zgoda. Polskie urzędy i firmy ją [href="http://securitystandard.pl/news/107001.html"](http://securitystandard.pl/news/107001.html) zdają się nie rozumieć/a_i, że SSL nie służy wyłącznie do ochrony przed podsłuchem, ale przede wszystkim do zagwarantowania, że klient łączy się autentycznym i zaufanym serwerem. Jeśli urząd taki jak Ministerstwo Finansów wystawia jakieś formularze petentom, to dobrze byłoby dopieścić ich maksymalnie pod względem dobrego samopoczucia, na przykład w postaci kłódki u dołu ekranu.

Z punktu widzenia analizy ryzyka a nie PR rozwiązanie w e-Deklaracjach jest poprawne, bo dane do bramki jednak idą po SSL. Bardziej uzasadnione byłoby podpisywanie wtyczki do e-Deklaracji (a ściślej tego instalatora EXE). Certyfikat do podpisywania kodu w GoDaddy kosztuje 200 USD rocznie, więc nie róbmy scen...

Średnio trafiony jest zarzut o stosowaniu 40-bitowego DES. Z pewnością jest to sprzeczne z "dobrymi praktykami inżynierskimi" oraz zaleceniami wszystkich możliwych instytucji z NIST na czele. Ale znajmy proporcje - nikt nie będzie łamał 40-bitowego DES (co jest nadal znacznie trudniejsze niż złamanie 128-bitowego RC4 w WEP) tylko po to, żeby podsłuchać cudzą deklarację podatkową. Najpierw ktoś musiałby mieć ku temu powód, a potem jest tysiąc prostszych sposobów (patrz ją [href="http://xkcd.com/538/"](http://xkcd.com/538/)) i pouczający rysunek z XKCD/a_i).

Na pewno brakuje publicznie dostępnej analizy ryzyka. To jest przypadłość wszystkich projektów w polskiej administracji publicznej, nie tylko e-Deklaracji. Urzednikom wydaje się zapewne, że jeśli nie napiszą w zamówionej za 200 tys. zł ekspertyzie o jakimś zagrożeniu, to nikt o nim nie będzie wiedział (np. że statyczne hasła są podatne na phishing). To wymaga rozwiązania systemowego oraz częstego korzystania z prawa do informacji publicznej, aż się nie nauczą że łatwiej samemu wystawić.

Pisze o tym z dwóch powodów. W naszej administracji publicznej działa obsesyjnie uwarunkowane lobby zwolenników niezwykle silnego, ale nieużywalnego "bezpieczeństwa wszystkiego" . Można dyskutować, czy chodzi ją [href="http://www.dziennik.krakow.pl/Artykul.100+M53a3acbb1c9.0.html"](http://www.dziennik.krakow.pl/Artykul.100+M53a3acbb1c9.0.html) i o zwykłą obsesję/a_i czy ją [href="http://blog.securitystandard.pl/news/342973.html"](http://blog.securitystandard.pl/news/342973.html) i o zwykłe pieniądze/a_i. Każda taka publikacja staje się pożywką dla lobby, które będzie ten artykuł drukować i używać jako argumentu dla konieczności wprowadzenia trzystopniowego uwierzytelnienia dla wszystkiego (ją [href="http://kononowicz.pl/polityka-wybory/179"](http://kononowicz.pl/polityka-wybory/179)) i by wszystko było tak bezpieczne, żeby nie było niczego/a_i). Nie chodzi o to, żeby nie pisać o dziurach, chodzi o to by nie pisać o nich "na szybko".

Po drugie, dziennikarze mają skłonność do przesadzania, bo z tego mają pieniądze. Kiedy pewna poczytna gazeta o wiarygodności proporcjonalnej do swojej ceny opublikowała tekst pod tytułem "Posłowie chcą zakazać przerwy" to nie zrobiła tego w ramach spisku, tylko dla przyciągnięcia uwagi czyli dla pieniędzy (a chodziło o to, żeby na pudełkach z tabletkami hormonalnymi pisać o skutkach ubocznych). Sam musiałem kiedyś wycofać swoją wypowiedź na etapie autoryzacji, kiedy dziennikarz mój "mało prawdopodobny problem z bezpieczeństwem" chciał przerobić na "katastrofę od której natychmiast umrze mnóstwo emerytów" (moja parafraza). Firma zajmująca się bezpieczeństwem nie powinna występować w takim kontekście.