



Wszyscy chyba pamiętamy historie StartCom urzędu certyfikacyjnego dostarczającego certyfikaty SSL, który nie tak dawno stracił status zaufanego jako centrum autoryzacyjne.

1 grudnia 2017 roku firma StartCom poinformowała swoich klientów o zawieszeniu działalności jako urząd certyfikacji. Cała sytuacja ma swoje podłoże w wydarzeniach mających swój początek w 2015 roku.

Wszystko zaczęło się od nadużyć ze strony WoSign, które to dopuściło się przewinień z punktu widzenia bezpieczeństwa użytkowników takich przeglądarek jak Mozilla czy Chrome. WoSign zarzucono między innymi:

- Duplikowanie numerów seryjnych certyfikatów
- Wykorzystywanie niedozwolonego algorytmu SM2 do generacji kluczy certyfikatów
- Przejęcie urzędu certyfikacji StartCom bez ujawnienia tej informacji.

Z uwagi na powiązania WoSign ze StartCom (kupienie StartCom w 2015, współdzielenie oprogramowania czy infrastruktury) firmy takie jak np. Mozilla postanowiły traktować je jako jeden urząd certyfikacji. Stąd w wyniku dochodzenia i zaistniałej sytuacji doszło do wprowadzenia braku zaufania w przeglądarkach jak Chrome czy FireFox dla certyfikatów StartSSL. Również później wydawane certyfikaty nie były traktowane jako zaufane przez dane przeglądarki.

StartCom zaproponowało plan naprawczy, restrukturyzację struktury organizacyjnej firmy i kompletne odcięcie od WoSign. Mimo to, według Mozilli przewinienia dotyczyły przeszłości, kiedy to StartCom należał do WoSign i firma postanowiła nie zmieniać decyzji o usunięciu zaufania względem StartCom.

StartCom mogło ubiegać się o ponowne dodanie do zaufanych po spełnieniu odpowiednich wymogów. Zgodnie z treścią maila wysłanego do klientów z 1.12.2017 StartCom zapewnia, że ich zdaniem zmiany zostały wprowadzone, a warunki zostały w spełnione. Mimo tego, zauważono, że ponowne dodanie ich certyfikatów do zaufanych przez popularne przeglądarki przebiega z wielkimi trudnościami. Z tego powodu firma postanowiła zawiesić działalność i od 1 stycznia 2018 nie będzie wydawać już nowych certyfikatów StartSSL. Firma pozostanie jedynie przy świadczeniu usług CRL i OCSP przez kolejne dwa lata. Jednocześnie zapewnia, że kontaktuje się z innymi urzędami certyfikującymi, aby dostarczyć klientom potrzebne certyfikaty. Proponuje również pomoc w znalezieniu alternatywy dla ich certyfikatu.



Czy StartCom uda się odzyskać reputację i powrócić do łask w roli urzędu certyfikacyjnego? Próbowano się starać, ale z tych działań nie wynikają żadne pozytywy dla StartCom. Stąd może się wydawać, że StartCom nie ma szans na ponowne funkcjonowanie na rynku. Warto również przypomnieć, że StartCom oferowało między innymi darmowe certyfikaty dla stron www. Na dzień dzisiejszy najlepszą alternatywą wydaje się być Let's Encrypt.

Poniżej załączamy oryginalny mail od StartCom z wyjaśnieniami całego zajścia z zawieszeniem działalności.

Dear customer,

As you are surely aware, the browser makers distrusted StartCom around a year ago and therefore all the end entity certificates newly issued by StartCom are not trusted by default in browsers.

The browsers imposed some conditions in order for the certificates to be re-accepted. While StartCom believes that these conditions have been met, it appears there are still certain difficulties forthcoming. Considering this situation, the owners of StartCom have decided to terminate the company as a Certification Authority as mentioned in Startcom's website.

StartCom will stop issuing new certificates starting from January 1st, 2018 and will provide only CRL and OCSP services for two more years.

StartCom would like to thank you for your support during this difficult time.

StartCom is contacting some other CAs to provide you with the certificates needed. In case you don't want us to provide you an alternative, please, contact us at [certmaster@startcomca.com](mailto:certmaster@startcomca.com)

Please let us know if you need any further assistance with the transition process. We deeply apologize for any inconveniences that this may cause.

Best regards,

StartCom Certification Authority