CERB

Silne dwuskładnikowe uwierzytelnienie użytkowników

Oprogramowanie CERB jest systemem umożliwiającym zastąpienie powszechnie wykorzystywanych haseł statycznych metodą silnego uwierzytelnienia dwuskładnikowego. To technika, która opiera się na zasadzie „coś masz i coś wiesz", tj. w celu bezpiecznego zalogowania się do danej usługi potrzebne są dwa elementy: hasło statyczne, znane tylko użytkownikowi oraz hasło jednorazowe, dostarczane przez „zewnętrzne źródło".

Wykorzystaj telefon komórkowy w procesie logowania
W systemie CERB rolę „zewnętrznego źródła", czyli drugiego składnika w procesie uwierzytelnienia, pełni telefon komórkowy. Wystarczy, że na telefonie zainstaluje się aplikację JavaToken, a telefon zamieni się w sprzętowy generator tokenów i haseł jednorazowych. Jeżeli telefon nie obsługuje technologii java, hasła jednorazowe mogą być przesyłane z wykorzystaniem technologii SMS.

Bez telefonu nie wychodzimy już z domu
Telefon komórkowy to obecnie przedmiot, który obok dokumentów, pieniędzy i kluczy, zawsze nosimy przy sobie. Innowacyjne podejście zawarte w systemie CERB pozwala zachować taki stan rzeczy i nie wymaga od użytkownika pamiętania o dodatkowych kartach kryptograficznych, kartach TAN czy sprzętowych tokenach. Wystarczy telefon komórkowy.

Funkcjonalność challenge-response. CERB to nie tylko hasła jednorazowe
W oferowanym rozwiązaniu zawarta została możliwość wykorzystania technologii challenge-response (zapytanie-odpowiedź). Jest to doskonała forma uwierzytelnienia wszelkich transakcji elektronicznych jak również forma bezpiecznego logowania użytkowników. Funckjonalność ta idelanie nadaje się do zastosowania w bankowości elektronicznej, serwisach webowych oraz aplikacjach gdzie istnieje możliwość „komunikacji z użytkownikiem" – system podaje ciąg znaków identyfikujących daną transakcję/proces, ciąg ten wpisywany jest do aplikacji JavaToken, po czym aplikacja podaje hasło zwrotne, które należy wpisać do systemu.

Zapomnij o wielu urządzeniach do różnych usług!
Ważną cechą oferowanego rozwiązania jest możliwość zastosowania tego samego telefonu komórkowego w kilku różnych środowiskach wykorzystujących system CERB. Środowiska te mogą być całkowicie od siebie niezależne tj. ten sam telefon może posłużyć do zalogowania się do sieci wewnętrznej, serwisu www, jak i wybranego banku elektronicznego. Użytkownik nie ma już konieczności noszenia wielu kart czy tokenów sprzętowych, z których każdy dedykowany jest do konkretnej usługi.

Główne korzyści

silne dwuskładnikowe bezpieczeństwo;

rozwiązanie sprawdzone przez kilka tysięcy użytkowników;

współpraca z liderami rynku sieciowego w tym m.in. z Crossbeam Systems, Cisco Systems, Nortel Networks, Check Point Software Technologies, Hewlett Packard;

wystarczy jeden telefon komórkowy by zalogować się do wielu różnych środowisk;

kilka możliwości bezpiecznego uwierzytelnienia: tokeny, hasła jednorazowe challenge-response;

jeden PIN (hasło statyczne) do wielu usług;

intuicyjna i łatwa obsługa JavaToken i SMSToken (generacja tokena jednym kliknięciem);

prosta administracja serwerem (WEB GUI lub linią komend);

możliwość dowolnego oskryptowania systemu;

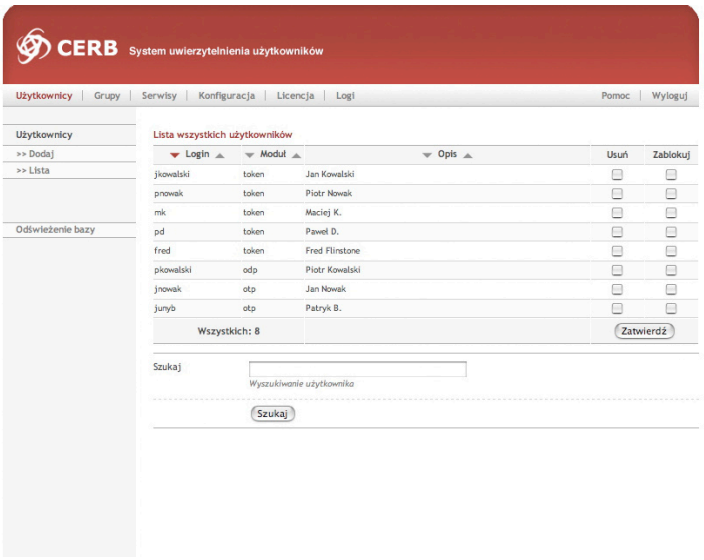
znacznie tańsze rozwiązanie w porównaniu z typowymi tokenami sprzętowymi, kartami TAN, PKI;

produkt tworzony i rozwijany w Polsce co gwarantuje możliwość uzyskania bardzo restrykcyjnych warunków serwisowych oraz możliwość modyfikacji pod kątem klienta.

CERB Silne dwuskładnikowe uwierzytelnienie użytkowników

Centralne zarządzanie użytkownikami
Administrator otrzymuje narzędzia umożliwiające centralne zarządzanie wszystkimi użytkownikami danego środowiska, przyznawanie i anulowanie praw dostępu jak również analizowanie całego odbywającego się ruchu związanego z dostępem do usług. Istnieje możliwość podziału użytkowników na grupy oraz przypisania im uprawnień do konkretnie wybranych serwisów. Dodatkowo wszystkim obiektom w systemie administrator może nadać dowolne charakterystyki – atrybuty.

Administracja systemem odbywa się z wykorzystaniem łatwego i wygodnego w obsłudze WEB GUI (panelu zarządzającego przez www) lub linii komend.



Bezpieczeństwo w zgodzie z łatwością obsługi
System CERB został zoptymalizowany szczególnie pod kątem bezpieczeństwa. Algorytmy w nim wykorzystane to znane i poważane standardy jak AES-256 i SHA-256, zapewniające najwyższy poziom ochrony przeprowadzanych tą metodą operacji. Hasła przechowywane na serwerze szyfrowane są zgodnie ze standardem PKCS#5v2.

Wykorzystanie silnego bezpieczeństwa nie wpłynęło w żaden sposób na wygodę i przyjazność użytkowania. Wszelkie procesy kryptograficzne są praktycznie niewidoczne dla obsługującego, a użytkownikom JavaToken wystarczy podstawowa wiedza dotycząca obsługi telefonu komórkowego.

Zastosowanie
System **CERB** wykorzystywany jest obecnie przez kilka tysięcy zadowolonych użytkowników. Współpraca z rozwiązaniami czołowych dostawców technologii informatycznych (m.in. Crossbeam Systems, Cisco Systems, Nortel Networks, Check Point Software Technologies, Hewlett Packard) pozwala na integrację systemu w bardzo wielu różnych środowiskach IT.

Poniżej przedstawiamy jedynie wybrane propozycje zastosowania systemu **CERB**:

- serwisy internetowe (współpraca z dowolnymi aplikacjami webowymi);
- banki elektroniczne, jako ochrona swojego konta bankowego lub jako potwierdzenie transakcji;
- sieci korporacyjne (w intranetach i extranetach jako kontrolowany dostęp do zasobów);
- w procesie uwierzytelnienia podczas ustanawiania kanałów VPN;
- w procesie logowania do systemów uniksowych;
- w systemach telefonii VoIP;
- w systemach sieci bezprzewodowych WiFi;
- oraz wszędzie tam gdzie w procesie uwierzytelnienia może zostać wykorzystany protokół RADIUS.

WHEEL

Wheel Sp. z o.o.
Ul. Świerszcza 72,
02-401 Warszawa

Tel.: +48 22 863 18 80
Fax: +48 22 863 40 69
e-mail: info@wheel.pl