

 Zawartość zarchiwizowana w dniu 2024-06-18



SEcure Cloud computing for CRITICAL infrastructure IT

Wyniki w skrócie

Architektura, narzędzia i mechanizmy pozwalające na bezpieczne stosowanie chmury obliczeniowej w zastosowaniach krytycznych

W oparciu o wytyczne techniczno-prawne opracowano zbiór narzędzi, mechanizmów i zaleceń dotyczących zabezpieczeń, aby uczynić chmurę obliczeniową bardziej przejrzystą, bezpieczną i odporną w przypadku wykorzystywania jej w krytycznych infrastrukturach i aplikacjach.



GOSPODARKA
CYFROWA



BEZPIECZEŃSTWO



© Melpomene, Shutterstock

Technologia cloud computing ułatwia wymianę wiedzy, tworzenie nowych usług oraz dostęp do informacji, ale jej stosowanie wiąże się z zagrożeniami i problemami dotyczącymi bezpieczeństwa. W ramach projektu SECCRIT (Secure cloud computing for critical infrastructure IT), finansowanego ze środków UE, badano technologie chmury obliczeniowej i związane z nimi zagrożenia wpływające na infrastrukturę krytyczną, aby zwiększyć bezpieczeństwo i odporność chmury.

Angażujący specjalistyczne instytucje i organizacje z Austrii, Finlandii, Niemiec, Grecji, Włoch, Hiszpanii i Zjednoczonego Królestwa projekt poświęcony był kilku obszarom badań, mającym poprawić bezpieczeństwo i odporność infrastruktur i

aplikacji o znaczeniu krytycznym.

Zespół przygotował w pierwszej kolejności katalog słabych punktów jako źródło danych do metodologii oceny ryzyka, przyczyniając się do rozwoju narzędzi oceny ryzyka oraz standaryzacji europejskiej w tej dziedzinie. Uczeń pracował nad specyfikacją, decyzjami i egzekwowaniem polityk na rzecz bezpiecznego zarządzania danymi w chmurze, a także modelem odporności obejmującym "wykrywanie anomalii jako usługę".

Innym ważnym celem było opracowanie narzędzi do ścieżek audytu i analizy przyczyn źródłowych, wśród których znalazły się prototypy oprogramowania open source. Zespół przygotował metodę oceny profilu kontroli jakości chmury wraz ze skryptami testowymi.

Komponenty oprogramowania narzędzia udoskonalono przy pomocy wytycznych dotyczących bezpieczeństwa, które pomagają interesariuszom infrastruktury krytycznych w korzystaniu z chmury, a także wytycznych zawierających zalecenia na temat odnośnych kwestii technicznych i prawnych. Od samego początku ważnym aspektem było spełnienie wymogów prawnych, ponieważ opracowane systemy muszą być zgodne z prawem, aby można je było stosować w praktyce. W tym celu w projekcie SECCRIT zastosowano podejście uwzględniające kwestie prawne dotyczące ochrony prywatności.

Oprócz opracowania i przetestowania wymienionych narzędzi i mechanizmów zespół przygotował 38 recenzowanych artykułów naukowych, a także zorganizował cztery warsztaty dla użytkowników oraz seminarium poświęcone bezpieczeństwu chmury. Prace te zostały też wykorzystane w dysertacjach studentów, wykładach i kolejnych projektach, a ponadto planuje się komercjalizację oprogramowania.

Zapewnienie bezpieczeństwa i odporności chmury dla infrastruktury krytycznych oznaczać będzie większą produktywność i wydajność firm oraz przemysłu. Działania te pomogą też podnieść jakość życia Europejczyków.

Słowa kluczowe

[Infrastruktura krytyczna](#)

[chmura obliczeniowa](#)

[SECCRIT](#)

[wykrywanie anomalii](#)

[odporność](#)

[bezpieczeństwo chmury](#)

Znajdź inne artykuły w tej samej dziedzinie zastosowania



Czy system robotyczny jest w stanie uratować pszczoły?

26 Maja 2023



Zintegrowany ekosystem zarządzania energią na potrzeby inteligentnych budynków

21 Lutego 2024



Splątanie uwięzionych jonów na dystansie przekraczającym 200 metrów

21 Lutego 2023



Przesyłanie informacji kwantowych między Alice i Charlie'em

17 Października 2022



Informacje na temat projektu

SECCRIT

Finansowanie w ramach

Specific Programme "Cooperation": Security

Identyfikator umowy o grant: 312758

Koszt całkowity

€ 4 801 715,00

Strona internetowa projektu 

Wkład UE

€ 3 397 319,00

Projekt został zamknięty

Data rozpoczęcia

1 Stycznia 2013

Data zakończenia

31 Grudnia 2015

Koordynowany przez

AIT AUSTRIAN INSTITUTE OF
TECHNOLOGY GMBH



Austria

Ten projekt został przedstawiony w...

MAGAZYN RESEARCH*EU



**Galileo applications: what
lies ahead**

Ostatnia aktualizacja: 7 Grudnia 2016

Permalink: <https://cordis.europa.eu/article/id/190642-architecture-tools-and-mechanisms-for-secure-cloud-computing-and-its-use-in-critical-applicat/pl>

European Union, 2025