HORIZON 2020

A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis

Wyniki w skrócie

Prostszy sposób zapobiegania cyberatakom

Nowe rozwiązanie wykorzystuje systemy świadomości sytuacyjnej oraz częściową automatyzację w celu wsparcia organów administracji publicznej i MŚP w wykrywaniu zagrożeń, ich kategoryzacji oraz podejmowaniu odpowiednich działań.

GOSPODARKA CYFROWA

BEZPIECZEŃSTWO

© Michael Traitov, Shutterstock

Cyberbezpieczeństwo jest coraz częściej postrzegane jako największe zagrożenie dla każdej firmy i organizacji na świecie. Pomimo że kolejne przepisy i regulacje, takie jak dyrektywa dotycząca bezpieczeństwa sieci i systemów informatycznych (NIS) czy ogólne rozporządzenie o ochronie danych (RODO), mają na celu poprawę cyberbezpieczeństwa, ich przestrzeganie może nastręczać wielu trudności. Dotyczy to w szczególności organów administracji publicznej oraz firm z sektora małych i średnich przedsiębiorstw, którym często brakuje środków na inwestycje w niezbędne najnowocześniejsze rozwiązania zapewniające bezpieczeństwo.

Aby wspomóc organy organów administracji publicznej, organizacje pozarządowe oraz małe i średnie przedsiębiorstwa w wykrywaniu zagrożeń cyberbezpieczeństwa oraz ochronie przed ich skutkami, zespół finansowanego przez Unię Europejską

projektu CS-AWARE (A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis) opracował zestaw prostych i stosunkowo tanich rozwiązań w zakresie cyberbezpieczeństwa oraz zwiększania świadomości dotyczącej tego zagadnienia.

„CS-AWARE to zbiór innowacyjnych rozwiązań pozwalających tym podmiotom na wykrywanie, kategoryzację oraz wizualizację incydentów związanych z cyberbezpieczeństwem w czasie rzeczywistym, wspomagając w ten sposób działania zapobiegawcze oraz łagodzenie skutków cyberataków", mówi Juha Röning, badacz Uniwersytetu w fińskim Oulu i koordynator projektu CS-AWARE.

Świadomość sytuacyjna

Podstawą projektu CS-AWARE jest element świadomości sytuacyjnej związanej z cyberbezpieczeństwem, który został opracowany z myślą o zgodności z istniejącymi i przyszłymi przepisami dotyczącymi tego zagadnienia. „Udostępnianie informacji na temat zagrożeń w cyberprzestrzeni przynosi szereg korzyści podmiotom, do których trafiają. Ponadto powszechnie uważa się, że jest to jedno z najważniejszych narzędzi pozwalających na walkę z cyberprzestępczością jakimi obecnie dysponujemy", wyjaśnia Röning. „Dzięki wykorzystaniu istniejących informacji dotyczących cyberbezpieczeństwa nasze rozwiązanie umożliwia wykrywanie incydentów oraz ich klasyfikację, a jednocześnie spełnia wszystkie wymagania dotyczące wymiany informacji wynikające z dyrektywy NIS oraz RODO", dodaje.

Pomimo stosunkowo dużego znaczenia, sama identyfikacja, pozyskiwanie oraz przechowywanie informacji o cyberzagrożeniach i incydentach nie jest wystarczające. „Prędkość generowania kolejnych informacji na temat cyberzagrożeń może być na tyle ogromna, że ani ludzki mózg, ani podstawowe systemy ochronne nie są w stanie sprostać wyzwaniu przetwarzania dużych zbiorów danych dotyczących incydentów", dodaje Röning. „Jesteśmy świadomi tego faktu, dlatego nasze rozwiązanie wykorzystuje złożone algorytmy decyzyjne, które pozwalają na identyfikację najbardziej prawdopodobnych zagrożeń, a następnie przesłanie informacji na ich temat specjalistom oraz innym zautomatyzowanym systemom w celu przetwarzania oraz łagodzenia ich możliwych skutków".

Rozwiązanie CS-AWARE pozwala na automatyzację znaczącej części procesu wykrywania cyberzagrożeń, jednak na całkowitą automatyzację musimy jeszcze poczekać. „Każda instytucja publiczna wykorzystuje inne systemy, co w praktyce uniemożliwia stworzenie jednego uniwersalnego i w pełni zautomatyzowanego rozwiązania", zauważa Röning. „Z tego powodu nasze rozwiązanie wykorzystuje analizę zależności opartą na miękkim myśleniu systemowym, która pozwala nam zidentyfikować najcenniejsze i najważniejsze elementy danego systemu w celu ich monitorowania".

Sprawdzone rozwiązania

Rozwiązanie CS-AWARE zostało wdrożone w ramach projektów pilotażowych i sprawdzone w realnych warunkach w greckiej Larissie oraz w Rzymie. Ponadto dzięki publikacjom naukowym oraz publicznemu udostępnieniu wyników badań zespół projektu przyczynił się również do rozwoju otwartego oprogramowania na potrzeby konkretnych technologii w zakresie cyberbezpieczeństwa.

Najważniejszym osiągnięciem projektu CS-AWARE było jednak zebranie doskonałego zespołu ekspertów, którzy obecnie skupiają się na komercjalizacji technologii opracowanej w ramach prac nad projektem, działając w nowo utworzonej spółce CS-Aware Corporation OÜ.

Słowa kluczowe

CS-AWARE | cyberatak | świadomość sytuacyjna | cyberbezpieczeństwo | dyrektywa na temat bezpieczeństwa sieci i systemów informatycznych | NIS | ogólne rozporządzenie o ochronie danych | RODO | cyberprzestępczość | duże zbiory danych

Znajdź inne artykuły w tej samej dziedzinie zastosowania

Roboty – pomagają czy przeszkadzają w zrównoważonym rozwoju?

8 Lipca 2022

Zniwelowanie luki między innowacjami w zakresie dużych zbiorów danych i ochroną ich prywatności

3 Lutego 2021

Uodparnianie globalnych łańcuchów dostaw na cyberzagrożenia

15 Listopada 2022

Automatyczne narzędzie ułatwia walkę z cyberprzestępstwami

15 Czerwca 2020

Informacje na temat projektu

CS-AWARE

Identyfikator umowy o grant: 740723

Strona internetowa projektu

DOI
10.3030/740723

Projekt został zamknięty

Finansowanie w ramach
Secure societies - Protecting freedom and security of Europe and its citizens

Koszt całkowity
€ 4 648 362,50

Wkład UE
€ 3 728 603,75

Koordynowany przez

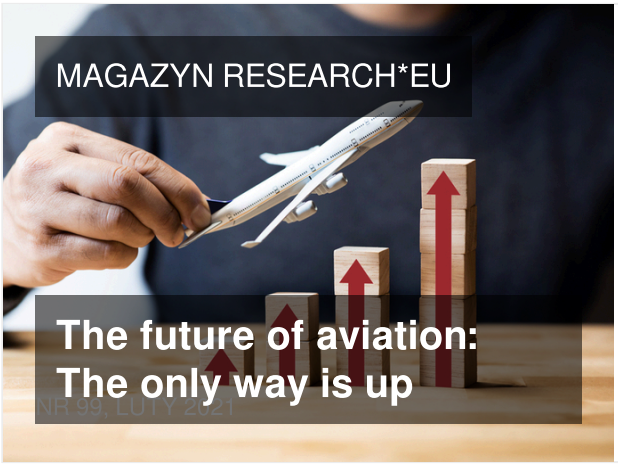
Data podpisania przez KE
26 Kwietnia 2017

OULUN YLIOPISTO
Finland

Data rozpoczęcia
1 Września 2017

Data zakończenia
31 Sierpnia 2020

Ten projekt został przedstawiony w...



Ostatnia aktualizacja: 3 Lutego 2021

Permalink: https://cordis.europa.eu/article/id/428899-a-simpler-way-of-preventing-cyberattacks/pl