Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control

Wyniki w skrócie

Intuicyjne rozwiązanie w zakresie cyberbezpieczeństwa dla domów podłączonych do sieci

Nowe, w pełni zautomatyzowane rozwiązanie w zakresie cyberbezpieczeństwa pomaga chronić inteligentne domy przed naruszeniem ochrony danych i innymi zagrożeniami.

GOSPODARKA CYFROWA

BEZPIECZEŃSTWO

© NicoElNino, Shutterstock

Kiedy słyszymy określenie „inteligentny dom”, często przychodzi nam na myśl, aby poprosić Google o aktualną prognozę lub Alexę o odtworzenie naszej ulubionej piosenki. Ale te urządzenia to tylko wierzchołek góry lodowej.

Prawdziwie inteligentny dom to taki, w którym zautomatyzowana technologia stosowana jest w najprzeróżniejszych miejscach, począwszy od urządzeń AGD, przez oświetlenie, ogrzewanie, alarmy, nagłośnienie i systemy, a skończywszy na roletach okiennych. Dzięki Internetowi rzeczy (IoT) te inteligentne urządzenia komunikują się ze sobą, tworząc w pełni zintegrowany ekosystem.

Jednak z coraz powszechniejszym wykorzystaniem inteligentnej technologii w domu wiąże się coraz większe ryzyko dotyczące cyberbezpieczeństwa. Ograniczenia tego ryzyka podjął się zespół finansowanego ze środków UE projektu GHOST.

Opracowuje on rozwiązanie w zakresie cyberbezpieczeństwa dla inteligentnych domów. „Założeniem inicjatywy GHOST jest stworzenie transparentnego środowiska cyberbezpieczeństwa, z którego będą mogli korzystać wszyscy Europejczycy żyjący w połączonym świecie”, mówi José Manuel Álvarez, kierownik projektu i zarazem kierownik ds. innowacji w Televés Corporation, firmie koordynującej projekt.

„Przy minimalnym wysiłku konsumenci będą mieli dostęp do informacji na temat zagrożeń związanych z cyberbezpieczeństwem, na jakie są narażeni, i będą mogli podejmować świadome decyzje w celu ich ograniczenia”.

Zabezpieczenia na poziomie korporacyjnym do użytku domowego

Celem projektu było wdrożenie wysoce użytecznego i skutecznego modelu bezpieczeństwa w inteligentnych domach. Aby zrealizować ten cel, naukowcy zastosowali zasady projektowania behawioralnego, tworząc rozwiązanie bezpieczeństwa zorientowane na użytkownika. „Architektura GHOST wspiera przyjazne dla bezpieczeństwa zachowania użytkowników, które są wprowadzone poprzez zastosowanie dyskretnego i zrozumiałego rozwiązania”, wyjaśnia Álvarez.

GHOST składa się z oprogramowania wbudowanego w bramy sieciowe inteligentnego domu. Korzystające z uczenia maszynowego i analizy danych rozwiązanie wykonuje analizę sieci i głęboką inspekcję pakietów w poszukiwaniu podejrzanych wzorców i złośliwych zachowań. GHOST wykorzystuje również blockchain do dalszego zwiększenia bezpieczeństwa inteligentnych domów dzięki wykorzystaniu odpowiednich inteligentnych umów.

„Dom z systemem GHOST zapewnia użytkownikowi analizę w czasie rzeczywistym wszystkich połączeń i danych wymienianych między podłączonymi urządzeniami i usługami zewnętrznymi”, dodaje Álvarez. „System powiadamia użytkownika o każdym podejrzanym połączeniu, gdy wymieniane są nowe dane lub gdy urządzenie przełącza się ze standardowego serwera”.

Rezultatem jest usługa ochrony na poziomie korporacyjnym, której można używać w domu.

Mechanizm samoobrony dla domu podłączonego do sieci

Uczestnikom projektu udało się stworzyć wysoce zautomatyzowany model inspekcji bezpieczeństwa oraz odporny, zdecentralizowany mechanizm samoobrony dla domu podłączonego do sieci. W ten sposób system GHOST daje użytkownikom kontrolę nad ich prywatnością i bezpieczeństwem.

„Dając konsumentom do dyspozycji wygodny zestaw narzędzi do kontroli, wykrywania i podejmowania decyzji w zakresie cyberbezpieczeństwa, przenieśliśmy nacisk z kontroli danych przychodzących na większą świadomość i kontrolę w zakresie danych wychodzących”, mówi Álvarez.

Rozwiązanie GHOST zostało przetestowane w ramach zakrojonych na szeroką skalę, długoterminowych prób przeprowadzonych w warunkach rzeczywistych, w tym w domach opieki i domach prywatnych w Norwegii, Rumunii oraz Hiszpanii.

Słowa kluczowe

GHOST, cyberbezpieczeństwo, dom podłączony do sieci, inteligentny dom, naruszenie ochrony danych, Internet rzeczy, IoT, uczenie maszynowe, blockchain

Znajdź inne artykuły w tej samej dziedzinie zastosowania

Webinaria na temat obliczeń wielkiej skali przyniosą korzyści środowiskom badawczym i przemysłowym w Europie i Ameryce Łacińskiej

Gdy technologia zapewnia ochronę

Analiza big data dla opornych

Wszechobecne oczy i uszy pomogą w ochronie europejskich portów

Informacje na temat projektu

GHOST

Identyfikator umowy o grant: 740923

Strona internetowa projektu

DOI
10.3030/740923

Projekt został zamknięty

Data podpisania przez KE
26 Kwietnia 2017

Data rozpoczęcia
1 Maja 2017

Data zakończenia
30 Kwietnia 2020

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

Koszt całkowity
€ 4 995 519,25

Wkład UE
€ 3 603 831,75

Koordynowany przez
TELEVES SA
Spain

Powiązane artykuły

POSTĘPY NAUKOWE

Biometria ważnym elementem nowego zestawu narzędzi z zakresu cyberbezpieczeństwa w służbie zdrowia

12 Października 2020

Ostatnia aktualizacja: 5 Października 2020

Permalink: https://cordis.europa.eu/article/id/422292-an-intuitive-cybersecurity-solution-for-the-connected-home/pl