Rozproszony algorytm analizy cyberbezpieczeństwa w sieci korporacyjnej

Streszczenie

Niniejsza rozprawa poświęcona jest ostatnio dynamicznie rozwijającej się dziedzinie teleinformatyki, jaką jest cyberbezpieczeństwo. W pracy skoncentrowano się na procesie zarządzania podatnościami, a w szczególności na metodach, które pozwalają na poprawienie bezpieczeństwa sieci teleinformatycznej poprzez udoskonalenie procesu priorytetyzacji podatności, wykorzystując wiedzę o monitorowanym środowisku.

W rozprawie zaproponowane zostały metody automatycznej priorytetyzacji podatności z wykorzystaniem ogólnodostępnych standardów oceny krytyczności oraz informacji o wadze zasobu z punktu widzenia organizacji. Celem pracy jest wyznaczenie grupy podatności krytycznych, wysokich oraz średnich, jak również określenie kolejności, w jakiej powinny one być naprawiane poprzez dodanie kroku w fazie definiowania działań naprawczych procesu zarządzania podatnościami. Dodatkowo w pracy zostały ujęte mechanizmy pozwalające na wykonywanie obliczeń dla przyrastającej ilości danych z wykorzystaniem metod skalowania dostępnych w nowoczesnych technologiach rozwoju oprogramowania.

Analiza uzyskanych wyników oraz badania przeprowadzone w rzeczywistych środowiskach teleinformatycznych potwierdziły przydatność zaproponowanych algorytmów. Ponadto, zaproponowano dalsze kierunki badań w zakresie analizy bezpieczeństwa oraz monitoringu badanych sieci korporacyjnych, przy wykorzystaniu informacji o znanych podatnościach.

Distributed algorithm for cybersecurity analysis in the corporate network

Summary

This dissertation is devoted to the dynamically developing field of ICT, which is cybersecurity. The work focuses on the vulnerability management process, in particular on methods that allow to improve the security of the ICT network by improving the vulnerability prioritization process, using knowledge regarding the monitored environment.

The dissertation proposes methods of automatic vulnerability prioritization implementing the generally available standards of criticality assessment and information regarding the importance of the asset from the organisation point of view. The aim of the work is to identify a group of critical, high and medium vulnerabilities that should be repaired in the first instance by adding an additional step in the phase of defining corrective actions in the vulnerability management process. In addition, the work includes mechanisms that allow to perform calculations for an increasing amount of data using scaling methods available in modern software development technologies.

The analysis of the obtained results and the research carried out in real ICT environments confirmed the usefulness of the proposed algorithms. In addition, further research directions were proposed in the field of security analysis and monitoring of the investigated corporate networks with the use of information on known vulnerabilities.