Securitate cibernetică: vulnerabilitățile sistemelor informatice ale viitorului

Autor: Ionuț-Daniel BARBU

Teza de doctorat analizează stadiul securității cibernetice actuale la nivel global, prezintă considerațiile personale referitoare la perspectivele de evoluție a amenințărilor și vulnerabilităților cibernetice și propune soluții de securizare aplicabile atât sistemelor informatice actuale, cât și celor din viitorul apropiat. Obiectivul principal al lucrării a fost reprezentat de dezvoltarea unei serii de produse compatibile și eligibile pentru securitatea cibernetică a viitorului prin studiul atacurilor informatice și al evoluției acestora pentru a înțelege impactul unei abordări proactive comparativ cu o abordare reactivă. Obiectivele secundare au constat în elaborarea unor analize teoretice, comparative împreună cu conceperea unor configurații hardware și aplicații software destinate minimizării impactului atacurilor cibernetice și optimizării costurilor în cadrul unor organizații. Am elaborat și aplicat un cadru de definire și analiză a riscului de securitate cibernetică în cadrul unei companii prin aplicarea metodei de defensivă stratificată (Defense in Depth). Contribuțiile au vizat resursa umană (gradul de conștientizare a securității cibernetice, profilul profesional al analistului cybersec) și soluțiile de îmbunătățire la nivelul managementului organizației (reducerea riscului, studiul comparativ al centrelor de securitate cibernetică de tip SOC și SIC). Printre contribuțiile la nivel tehnic subliniez sistemul de analiză a atacurilor și atacatorilor pe baza unei rețele de honeypot-uri, studiul impactului unor vulnerabilități precum Buffer Overflow sau Heartbleed și o soluție de detecție a unor forme de malware precum APT sau ransomware. Sunt estimați vectorii de atac specifici perioadei imediat următoare și sunt identificate câteva priorități cărora organizațiile vor trebui să le acorde atenție în vederea reluării și adaptării activităților la o „nouă normalitate" în contextul complex generat de pandemia de coronavirus.

Cyber Security: The Vulnerabilities of Future Information Systems

Author: Ionuț-Daniel BARBU

The PhD thesis analyzes the current state of cyber security from a global perspective, presents personal considerations regarding the prospects for the evolution of cyber threats and vulnerabilities and proposes security solutions applicable to both current and near-future information systems. The main purpose of the research was to develop a series of compatible and eligible products and services for the cyber security environment of the future by studying cyber-attacks and their evolution to understand the impact of a proactive approach compared to a reactive approach from a defensive point of view. The secondary objectives consisted in the elaboration of theoretical, comparative analysis applied on various hardware configurations and software applications designed to minimize the impact of the cyber-attacks and to optimize the costs within the studied organizations. As a consequence, a framework for defining and analyzing cyber security risk within a company by applying the method of layered defense (Defense in Depth) was developed and applied. The contributions focused on human aspect (cybersecurity awareness, professional profile of the cybersec analyst) as well as improvement solutions at the management level of the organization (risk mitigation, comparative study of cyber security centers SOC vs. SIC) with the aim of reducing the attack surface. Among the contributions at the technical level it is worth highlighting the cyber-attacks and attackers analysis system based on a interactive honeypot network, the study of the impact of vulnerabilities including Buffer Overflow or Heartbleed and a solution for detecting various forms of malware such as APT or ransomware. Finally, as the evolving threat landscape shifted in the context of the COVID-19 pandemic, the organizations will need to leverage a tailored approach to addressing the challenges of the new normal.