Kevin Daimi
Cathryn Peoples *Editors*

Advances in Cybersecurity Management

Springer

Advances in Cybersecurity Management

Kevin Daimi • Cathryn Peoples
Editors

Advances in Cybersecurity Management

Springer

Editors
Kevin Daimi
University of Detroit Mercy
Detroit, MI, USA

Cathryn Peoples
Ulster University
Newtownabbey, UK

ISBN 978-3-030-71380-5   ISBN 978-3-030-71381-2 (eBook)
https://doi.org/10.1007/978-3-030-71381-2

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Regardless of our technical ability in general, it is imperative to have some degree of competency in relation to cybersecurity—if we are online, we are all potential victims of a cybersecurity attack. However, as with any skill, we all have varying ability to exploit this competency. The extent to which any of us needs to be cybersecurity-aware varies depending on the role we play in the online world, and the position we fill in relation to a network and its supported systems and services. Those who are closer to the design and development of a network system will have different needs to those who are maintaining systems, selling systems, and using systems.

There are a variety of frameworks in place which support users and organizations in applying security techniques to protect themselves, their systems and applications, and their networks. The Object Management Group as one example has produced a series of cybersecurity standards. The European Commission, which is involved in working towards a cybersecurity initiative is another example. Nonetheless, despite all of these efforts, the cost of cyberattacks is continuing to grow. A report by Accenture in 2020 describes that the number of organizations spending more than 20% of their IT budget on cybersecurity has doubled in the last 3 years. Furthermore, 69% of organizations say that the cost of staying ahead of the attacks is unsustainable.

A gap therefore continues to exist in relation to the consideration of cybersecurity provisioning. The contents of **Advances in Cybersecurity Management** book contribute to international cybersecurity initiatives. It is relevant that the authors contributing chapters to this book come from a variety of backgrounds and experiences, helping to provide a range of perspectives with regard to the cybersecurity challenge. Furthermore, this book contains chapters from an internationally distributed author base, another important point to make, given that our perceptions and experiences in relation to cybersecurity vary based on our location worldwide.

This book is organized into three parts: The first part involves *Network and Systems Security Management,* the second concerns *Vulnerability Management,* and the third deals with *Identity Management and Security Operations*. Below, we present a brief overview of the book chapters.

Relevant to the nature of attacks in our networks today, an overview of a range of SQL injection attacks, with specific attention given to the focus on mitigation strategies, is provided. Identity management is the focus in another chapter. A framework to visualize cyberattacks, referred to as VizAttack, is further discussed.

In terms of cyberattacks to which organizations are exposed, a chapter communicates an important message that security awareness needs to be prevalent across an organization. In response to this, a gamification strategy is considered as an approach to prepare an organization for attacks. Further chapter considers the management of cybersecurity challenges in an organization, specifically from the perspective of industry.

In relation to modern day applications, a search engine is presented, which is applicable on a domain-specific approach, in recognition of the fact that cybersecurity information will have variable importance depending on the domain in which it is applied. Other authors consider techniques to exploit an online app, with a view to understanding the ways that they need to be made more secure. Recommendation of a social network analyzer is made in another chapter, with the goal of understanding if a friend is actually a friend, or if they have a more fraudulent intention when making the friend request. Further chapters consider the security metrics needed to support vehicular networks, and a protocol to support the operations of remote health monitoring applications.

Risk identification and management is an important part of dealing with cyberattacks. A number of authors contributed chapters to cover this area including the management of risk in relation to cybersecurity attacks, the use of biometrics to support risk mitigation in enterprises, a framework for managing risks in enterprises, and investigating the cycle of managing risks. Given the cost of security breaches, effective risk management is seen as critical, and opportunities for pre-emptive detection of the occurrence of risks is seen as being critical. Related to this, a chapter provides a history of security attacks, with a view to highlighting that it is important to analyze the traffic in the network in addition to the user behavior. In parallel with this concept, further chapter recognizes that the detection of security attacks from traffic flows will take place once the network begins to be compromised. Pre-emptive identification could be helpful, and the authors subsequently make a proposal to use the common characteristics of the people who attack to predict where problems may occur in the network.

While approaches can be made to manage risks, these will not be guaranteed, and the attacks themselves need to be managed. An author presents a recommender system to manage security using a rating approach, and a different author discusses agent-based modelling of entity behavior in cybersecurity.

Cyberattacks have become more prevalent recently, in the period of Covid-19. Related to this, some book chapters consider cybersecurity attacks during Covid-19. Going beyond this, other chapter discusses the cybersecurity challenges in the cloud after Covid-19, in recognition of rapid uptake in the number of cloud users and value of operating in the cloud. Furthermore, an argument is presented in relation to the need to plan cybersecurity techniques to be efficient due to the limited processing capabilities of hardware to respond to demand.

Based on the historical evidence that we are aware of in relation to cybersecurity attacks to date, the goalposts of security attacks will continue to move, and we will continue to require novel ways to both identify and response to cyberattacks. We hope that this book will provide valuable ideas on the “whats” and “whys” of cyberattacks, and that it supports readers in their knowledge and understanding of this complex field.

Detroit, MI, USA — Kevin Daimi
Newtownabbey, UK — Cathryn Peoples

Acknowledgments

The *Advances in Cybersecurity Management* book would not have been possible without the teamwork, encouragement, and support of many people. We would like to first acknowledge the authors of all chapters in this book, who contributed their knowledge and expertise in Cybersecurity Management. We are also grateful to the hard work of all chapter reviewers, who are listed below. Finally, we would like to express our gratitude to Mary James, Zoe Kennedy, and Brian Halm at Springer for their kindness, courtesy, professionalism, and support.

Jacques Bou Abdo, University of Nebraska at Kearney, USA
Mohammed Akour, Yarmouk University, Jordan
Abeer Alsadoon, Charles Sturt University, Australia
Roberto O. Andrade, Escuela Politécnica Nacional, Ecuador,
Allen Ashourian, ZRD Technology, USA
Sumitra Binu, Christ University, India
Khalil Challita, Notre Dame University-Louaize, Lebanon
Ralf Luis de Moura, Operational Technology Architecture, Brazil
Kevin Daimi, University of Detroit Mercy, USA
Ioanna Dionysiou, University of Nicosia, Cyprus
Guillermo Francia III, University of West Florida, USA
Mikhail Gofman, California State University of Fullerton, USA
Diala Abi Haidar, Jeddah International College, Saudi Arabia
Mary Ann Hoppa, Norfolk State University, USA
Gurdip Kaur, University of New Brunswick, Canada
Irene Kopaliani, Princeton University, USA
Arash Habibi lashkari, University of New Brunswick, Canada
Edison Loza-Aguirre, Escuela Politécnica Nacional, Ecuador
Doug Millward, University of Essex, UK
Esmiralda Moradian, Stockholm University, Sweden
Renita Murimi, University of Dallas, USA
Mais Nijim, Texas A&M University-Kingsville, USA
Kendall E. Nygard, North Dakota State University, USA

Nkaepe Olaniyi, Kaplan Open Learning, UK
Saibal K Pal, Defense R&D Organization, India
Cathryn Peoples, Ulster University, UK
Daniela Pöhn, Universität der Bundeswehr München, Germany
Karpoor Shashidhar, Sam Houston State University, USA
Nicolas Sklavos, University of Patras, Greece

Contents

Part I Network and Systems Security Management

Part II Vulnerability Management

Part III Identity Management and Security Operations