

SpringerBriefs in Applied Sciences and Technology
Computational Intelligence

**Gururaj H L · Spoorthi M · Vinayakumar Ravi ·
Shreyas J · Kumar Sekhar Roy**

Securing the Future

Introduction to Zero Trust
in Cybersecurity

SpringerBriefs in Applied Sciences and Technology

Computational Intelligence

Series Editor

Janusz Kacprzyk, Systems Research Institute, Polish Academy of Sciences,
Warsaw, Poland

SpringerBriefs in Computational Intelligence are a series of slim high-quality publications encompassing the entire spectrum of Computational Intelligence. Featuring compact volumes of 50 to 125 pages (approximately 20,000-45,000 words), Briefs are shorter than a conventional book but longer than a journal article. Thus Briefs serve as timely, concise tools for students, researchers, and professionals.

Gururaj H L · Spoorthi M · Vinayakumar Ravi ·
Shreyas J · Kumar Sekhar Roy

Securing the Future

Introduction to Zero Trust in Cybersecurity

 Springer

Gururaj H L
Department of Information Technology
Manipal Institute of Technology Bengaluru
Manipal Academy of Higher Education
Manipal, Karnataka, India

Spoorthi M
Department of Information Science
and Engineering
Vidhyavardhaka College of Engineering
Mysuru, Karnataka, India

Vinayakumar Ravi
Center for Artificial Intelligence
Prince Mohammad Bin Fahd University
Khobar, Saudi Arabia

Shreyas J
Department of Information Technology
Manipal Institute of Technology Bengaluru
Manipal Academy of Higher Education
Manipal, Karnataka, India

Kumar Sekhar Roy
Department of Computer Science
and Engineering
Manipal Institute of Technology Bengaluru
Manipal Academy of Higher Education
Manipal, Karnataka, India

ISSN 2191-530X ISSN 2191-5318 (electronic)
SpringerBriefs in Applied Sciences and Technology
ISSN 2625-3704 ISSN 2625-3712 (electronic)
SpringerBriefs in Computational Intelligence
ISBN 978-3-031-63780-3 ISBN 978-3-031-63781-0 (eBook)
<https://doi.org/10.1007/978-3-031-63781-0>

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2024

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

If disposing of this product, please recycle the paper.

Preface

This book is a descriptive summary of **Securing the Future: Introduction to Zero Trust in Cybersecurity** with various case studies from diverse authors across the globe.

The authors of Chapter 1 elaborated foundations of cybersecurity and the introduction of the Zero Trust model is at the vanguard of this revolutionary process. The core ideas of Zero Trust, a cutting-edge cybersecurity approach that calls into question network trust and mandates constant user identity, device, and application verification, are examined. And also emphasizes the critical role that Zero Trust plays in strengthening defenses, adjusting to changing cybersecurity problems, and safeguarding the digital future as enterprises navigate a constantly changing threat landscape.

In Chapter 2, authors have discussed the Zero Trust in detail including Core principles of the zero-trust model and The Need for Zero Trust. This chapter will serve as a primer for researchers to assimilate the use of Zero Trust which is a security framework that mandates that before granting or retaining access to applications and data, all users whether inside or outside the organization's network must be verified, approved, and regularly evaluated for security configuration and posture.

The authors of Chapters 3 and 4 provide an overview of zero-trust network implementation, characteristics, types, components, benefits, analytical tools and technologies, and most recent insights. A case study demonstrates the importance of zero-trust network adoption for cloud.

The authors of Chapters 5 and 6 discuss the compliance and governance in zero trust and Case Study of Building a Zero Trust Architecture for Industrial Environment. The authors of Chapters 7 elaborated the Zero Trust awareness, The Significance of User Education and Awareness, cyberattack types that impact K-12 institutions and Implementing Zero Trust in K-12 institutions.

The authors of Chapters 8 focused on difficulties they encountered like Complex implementation, Integrating security silos and legacy systems, and many more when implementing zero trust and also discussed the Future scope.

Bengaluru, India

Mysuru, India

Khobar, Saudi Arabia

Bengaluru, India

Bengaluru, India

Gururaj H L

Spoorthi M

Vinayakumar Ravi

Shreyas J

Kumar Sekhar Roy

Contents

1 Foundations of Cybersecurity	1
1.1 Overview	1
1.2 History of Internet and Computer Networks	2
1.3 Evolution of Cyber Threats	3
1.3.1 Rise of Malware	4
1.3.2 Interconnected Networks and Exploitation	4
1.3.3 Advanced Persistent Threats (APTs)	4
1.3.4 Exploitation of Zero-Day Vulnerabilities	4
1.3.5 Collaboration and Information Sharing	4
1.3.6 Artificial Intelligence (AI) Integration	5
1.4 The Dynamic Nature of Cyber Threats	5
1.5 Traditional Security Models and Their Limitations	7
1.5.1 Security Based on Perimeters	7
1.5.2 Network Segmentation	7
1.5.3 Firewall and Antivirus Solutions	8
References	8
2 Introduction to Zero Trust	11
2.1 Introduction to Zero Trust	11
2.1.1 Maturity Milestones	13
2.1.2 The Need for Zero Trust	17
2.2 Core Principles of the Zero-Trust Model	17
References	20
3 Implementing Zero Trust Networks	23
3.1 Trust in Zero Trust	23
3.1.1 Core Tenets of the Zero Trust Security Model	24
3.2 Implementation Challenges	28
References	29

- 4 Zero Trust for Cloud** 31
 - 4.1 What Is Zero Trust for Cloud? 31
 - 4.2 Why Companies Need ZT? 32
 - 4.3 Five-Step Process to Implement Zero Trust in the Cloud 34
 - 4.4 Zero Trust in the Cloud Can Be Used in the Following Use Cases .. 35
 - References 36
- 5 Compliance and Governance in Zero Trust** 39
 - 5.1 Overview of the Issues with Private Content Governance 40
 - 5.1.1 Managed Security Service Providers’ (MSSPs’) Function ... 40
 - 5.1.2 Understanding Cybersecurity Concepts in Relation to Private Content Governance 41
 - 5.1.3 Strong Private Content Governance’s Advantages 42
 - 5.2 Zeroing in on Security: The Vital Role of Governance and Compliance in Zero Trust 42
 - References 44
- 6 Applications & Case Studies of Successful Zero Trust** 47
 - 6.1 Case Study: Building a Zero Trust Architecture for Industrial Environment 47
 - 6.2 Google BeyondCorp 49
 - 6.2.1 Architecture of the BeyondCorp Infrastructure Components 50
 - 6.3 Cisco’s Zero Trust Architecture 52
 - 6.3.1 Zero Trust Security Frameworks 53
 - 6.4 DZ Bank Builds Zero Trust Security Strategy with CyberArk 56
 - 6.5 Zero Trust and Other Financial Entities 58
 - 6.6 Securing Remote Access with Zero Trust 59
 - References 62
- 7 Zero Trust Awareness: Creating a Culture Aware of Security** 65
 - 7.1 Zero Trust: The Significance of User Education and Awareness 66
 - 7.2 Password Vulnerabilities 66
 - 7.3 Clicking Dangerous Links 66
 - 7.4 Using Public WiFi 67
 - 7.5 Overcoming Obstacles: Techniques for Training Programs with Zero Trust 67
 - 7.5.1 Cyberattack Types that Impact K—12 Institutions 70
 - 7.5.2 Implementing Zero Trust in K—12 Institutions 72
 - 7.5.3 Invest in Zero Trust for Your Institution 72
 - References 73