

# Microsoft Azure Security Infrastructure



Yuri Diogenes

Dr. Thomas W. Shinder

Debra Littlejohn Shinder

Foreword by Mark Russinovich, Chief Technology Officer, Microsoft Azure

# Microsoft Azure Security Infrastructure

Yuri Diogenes  
Dr. Thomas W. Shinder  
Debra Littlejohn Shinder

# Microsoft Azure Security Infrastructure

## Table of Contents

Cover

Title Page

Copyright Page

Acknowledgments

Contents

Foreword

Introduction

Chapter 1 Cloud security

- Cloud security considerations

  - Compliance

  - Risk management

  - Identity and access management

  - Operational security

  - Endpoint protection

  - Data protection

- Shared responsibility

  - Cloud computing

  - Distributed responsibility in public cloud computing

- Assume breach and isolation

- Azure security architecture

- Azure design principles

Chapter 2 Identity protection in Azure

# **Table of Contents**

## Authentication and authorization

- Azure hierarchy

- Role-Based Access Control

## On-premises integration

- Azure AD Connect

- Federation

## Suspicious activity identification

## Identity protection

- User risk policy

- Sign-in risk policy

- Notification enabling

- Vulnerabilities

## Multi-Factor Authentication

- Azure Multi-Factor Authentication implementation

- Azure Multi-Factor Authentication option configuration

## Chapter 3 Azure network security

### Anatomy of Azure networking

- Virtual network infrastructure

- Network access control

- Routing tables

- Remote access (Azure gateway/point-to-site VPN/ RDP/Remote PowerShell/SSH)

- Cross-premises connectivity

- Network availability

- Network logging

- Public name resolution

- Network security appliances

- Reverse proxy

### Azure Network Security best practices

# **Table of Contents**

- Subnet your networks based on security zones
- Use Network Security Groups carefully
- Use site-to-site VPN to connect Azure Virtual Networks
- Configure host-based firewalls on IaaS virtual machines
- Configure User Defined Routes to control traffic
- Require forced tunneling
- Deploy virtual network security appliances
- Create perimeter networks for Internet-facing devices
- Use ExpressRoute
- Optimize uptime and performance
- Disable management protocols to virtual machines
- Enable Azure Security Center
- Extend your datacenter into Azure

## **Chapter 4 Data and storage security**

- Virtual machine encryption

- Azure Disk Encryption

- Storage encryption

- File share wire encryption

- Hybrid data encryption

  - Authentication

  - Wire security

  - Data at rest

- Rights management

- Database security

  - Azure SQL Firewall

  - SQL Always Encrypted

  - Row-level security

  - Transparent data encryption

# **Table of Contents**

Cell-level encryption

Dynamic data masking

## **Chapter 5 Virtual machine protection with Antimalware**

Understanding the Antimalware solution

Antimalware deployment

Antimalware deployment to an existing VM

Antimalware deployment to a new VM

Antimalware removal

## **Chapter 6 Key management in Azure with Key Vault**

Key Vault overview

App configuration for Key Vault

Key Vault event monitoring

## **Chapter 7 Azure resource management security**

Azure Security Center overview

Detection capabilities

Onboard resources in Azure Security Center

Apply recommendations

Resource security health

Respond to security incidents

## **Chapter 8 Internet of Things security**

Anatomy of the IoT

Things of the world, unite

Sensors, sensors everywhere

Big data just got bigger: TMI

Artificial intelligence to the rescue

IoT security challenges

IoT: Insecure by design

# **Table of Contents**

Ramifications of an insecure IoT

IoT threat modeling

Windows 10 IoT and Azure IoT

Windows 10 IoT editions

Azure IoT Suite and secure Azure IoT infrastructure

## **Chapter 9 Hybrid environment monitoring**

Operations Management Suite Security and Audit solution overview

Log Analytics configuration

Windows Agent installation

Resource monitoring using OMS Security and Audit solution

Security state monitoring

Identity and access control

Alerts and threats

## **Chapter 10 Operations and management in the cloud**

Scenario

Design considerations

Azure Security Center for operations

Azure Security Center for incident response

Azure Security Center for forensics investigation

Index

About the authors

Free eBooks

Survey